dLAN® pro 500 Wireless+

devolo

The Network Innovation

devolo dLAN® pro 500 Wireless+

© 2013 devolo AG Aachen (Germany)

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. devolo shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from devolo. We reserve the right to make any alterations that arise as the result of technical development.

Trademarks

HomePlug® is a registered trademark of HomePlug Powerline Alliance.

Linux® is a registered trademark of Linus Torvalds.

Ubuntu®is a registered trademark of Canonical Ltd.

Mac® and Mac OS X® are registered trademarks of Apple Computer, Inc.

Windows® and Microsoft® are registered trademarks of Microsoft, Corp.

Wi-Fi®, Wi-Fi Protected Access™, WPA™, WPA2™ and Wi-Fi Protected Setup™ are registered trademarks of the Wi-Fi Alliance®.

devolo, dLAN®, Vianect® and the devolo logo are registered trademarks of devolo AG.

All other names mentioned may be trademarks or registered trademarks of their respective owners. Subject to change without notice. No liability for technical errors or omissions.

devolo AG

Charlottenburger Allee 60

52068 Aachen

Germany

www.devolo.com

Aachen, September 2013

Contents

1 Preface 7
1.1 Thank you for placing your trust in this devolo product 7
1.1.1 About this manual 7
1.2 CE conformity 8

2 Introduction 9
2.1 What exactly is dLAN? 9
2.2 What is WLAN? 9
2.3 What is VLAN? 9
2.4 dLAN pro 500 Wireless+ 10
2.5 Sample applications 11
2.5.1 dLAN pro 500 Wireless+ as a WLAN access point 11
2.5.2 dLAN pro 500 Wireless+ as a WLAN client 13
2.5.3 dLAN pro 500 Wireless+ and VLAN 14

3 Initial use 17
3.1 Package contents 18
3.2 System requirements 18
3.3 Functions 19
3.3.1 Control lamps 19
3.3.2 Buttons 21
3.3.3 Network jacks 23
3.3.4 Wi-Fi antennas 23
3.4 Connecting the dLAN pro 500 Wireless+ 23
3.4.1 Software for Windows and Linux 24

4 Network configuration 25
4.1 Calling up the built-in configuration interface 25
4.2 Menu description 25
4.3 Status overview 26

4.3.1 dLAN status 28
4.3.2 WLAN status 28
4.3.3 Ethernet status 29
4.4 Device configuration 30
4.4.1 Device security 31
4.4.2 Network settings 33
4.4.3 dLAN settings 35
4.4.4 Time server 37
4.4.5 LED settings 38
4.5 WLAN configuration 38
4.5.1 Basic settings 39
4.5.2 WLAN time control 41
4.5.3 RADIUS server 43
4.5.4 Parental controls 43
4.5.5 WiFi Move Technology 45
4.5.6 dLAN pro 500 Wireless+ as Access point 46
4.5.7 Guest account 53
4.5.8 Wi-Fi Protected Setup (WPS) 56
4.5.9 dLAN pro 500 Wireless+ as a WLAN client 58
4.6 VLAN configuration 61
4.6.1 Create VLAN 63
4.6.2 Overview of configured VLANs 63
4.6.3 VLAN port settings 64
4.7 Management 66
4.7.1 Resetting the configuration 67
4.7.2 Saving a configuration file 68
4.7.3 Restoring a configuration 69
4.7.4 Update firmware 69

5 dLAN pro network 71
5.1 Security in the dLAN 71
5.2 dLAN pro network encryption at the touch of a button 71
5.3 dLAN AVpro manager 75

6 Appendix 77
6.1 Bandwidth optimization 77
6.2 Important safety instructions 78
6.3 Disposal of old devices 79
6.4 Warranty conditions 79

1 Preface

1.1 Thank you for placing your trust in this devolo product

devolo dLAN business solutions are a favourably priced option for using the power grid infrastructure in a building to establish a broadband IP network. The advantage this brings is obvious: no new cables have to be laid – expenditure and costs remain low.

The dLAN pro 500 Wireless+ is devolo's innovative access point for mobile as well as stationary network devices in a professional environment. Positioning anywhere in a building is possible due to the flexibility of dLAN pro networking over an existing power line: even areas without a network connection are perfectly integrated this way.

1.1.1 About this manual

After an introduction to "dLAN", "WLAN" and "VLAN" basics in **Chapter 2**, **Chapter 3** will cover successfully setting up your dLAN pro 500 Wireless+. **Chapter 4** describes in detail the setting options of the built-in configuration interface and thereby also access to the dLAN, VLAN and WLAN. For information on configuring the dLAN pro network, please see **Chapter 5**. Information about product safety and environmental compatibility of the device and our warranty terms can be found in **Chapter 6** and conclude the manual.

You can find the technical data for the dLAN pro 500 Wireless+ in the product information sheet on the enclosed product CD.

Description of the symbols

Here we briefly describe the meaning of the symbols used in this manual.

Very important note. Failure to observe this note may result in damage.

Important note that should be observed.

Additional information, background material and configuration tips for your device.

If you have any further ideas or suggestions related to our products, please don't hesitate to contact us at support@devolo.com!

devolo on the Internet

For detailed information on our products, visit www.devolo.com.

The area **dLAN for business projects** not only contains product descriptions and documentation, but also updates of devolo software and your device's firmware.

We especially recommend the descriptions of the "dLAN pro network," which are arranged according to **Application**, **Sectors** and **Integration**, where you can find lots of interesting background information.

1.2 CE conformity

CE 0680

This product complies with the technical requirements of the directive 1999/5/EC (R&TTE) and the other relevant provisions of the FTEG, and it is designed for use in the EU and Switzerland. The product is class A equipment. Class A devices may cause interference when used in residential environments.

"99/05/CE" (R&TTE directive) is a directive similar to the EMC directive. It applies to radio equipment and telecommunication terminal equipment.Observance of these directives is verified by the use of harmonized European norms.
For the CE declaration for this product, refer to the accompanying product CD under **CE**.

2 Introduction

dLAN is an intelligent, secure technology that lets you set up a home network easily, quickly and economically via your household electrical wiring, without the need for complex and expensive dedicated cabling. The available performance and effort required for the installation also compares favourably to traditional methods.

2.1 What exactly is dLAN?

dLAN (**d**irect **L**ocal **A**rea **N**etwork) uses the household power grid to transfer data between computers equipped with suitable adapters and other network components. As a result, any power outlet can be used as a network access point. The data is modulated prior to transfer and sent as a signal via household power lines. State-of-the-art technology ensures that the power and data networks do not interfere with one another. Networking via dLAN is fast and secure. The data is encrypted using a key to prevent interception by third parties.

2.2 What is WLAN?

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) refers to the use of radio technology to network computers and other devices. While it is possible to wirelessly connect computers in pairs (peer-to-peer, p2p), a central access point is required to set up a network of multiple devices. Such access points are frequently combined in a single device with modems for Internet access and routers to manage network traffic.

The wireless network established by an access point using a specific channel (from 1 to 140) and name (SSID) has a limited range. The range of the access point, which is also known as a "radio cell", is impeded by building walls. In some cases, stable connections are often only possible between WLAN devices within a single room.

As it is not possible to rely on hardware such as network cables (in a LAN) or household wiring (in a dLAN) to control access to a WLAN, wireless networking naturally presents special security challenges. WLANs therefore use a number of security measures, such as a concealed network name, data encryption and access control via the MAC addresses of the network adapters.

2.3 What is VLAN?

A **VLAN** (**V**irtual **L**ocal **A**rea **N**etwork, IEEE 802.1Q) is a logical, self-enclosed, local network – unlike a physical (switched) network. **VLANs** divide **physical** net-

works into multiple **logical, independent** networks. They optimise data distribution and make it easier to set up network architecture that is more secure and arranged more clearly.

Using VLANs prevents the need for complicated physical wiring. This gives you greater spatial flexibility and saves you having to purchase multiple costly individual devices (e.g. routers, switches).

Different criteria can be used for mapping to VLANs, such as port assignments, addresses, port numbers and protocols. The dLAN pro 500 Wireless+ allows VLANs to be mapped by port and/or access point. Other mapping methods by third-party devices using "VLAN tags" are also supported. In addition, it is possible to prioritise data traffic in the VLAN configuration.

2.4 dLAN pro 500 Wireless+

- Innovative access point for network-compatible terminal devices; whether dLAN, WLAN or classic network cable: every device can be connected!
- The dLAN powerline technology uses the internal power line and thus enables flexible positioning of the dLAN pro 500 Wireless+ everywhere in the building.
- Areas without network cables are integrated perfectly; alternatively, an existing network is ideally extended.
- Developed for use in businesses; already tried and tested in a multitude of sectors such as offices and production.
- Easy set-up of WLAN zones (WLAN access points and wireless hotspots) with support of the WLAN IEEE 802.11n high-speed standard.
- Lowering the transmitting power—e. g. if you do not require a large range. For example, if you are in the same room as the dLAN pro 500 Wireless+.
- Separation of user groups and granular access control through access points (Multi SSID) and VLAN.
- Ideal as a comprehensive, fast and stable network solution or for support of existing network infrastructure.
- 500 Mbps (gross) connection for fast data transmission via dLAN, 300 Mbps (gross) in WLAN operation (IEEE 802.11n standard).
- Professional WLAN security management with support for WPA/WPA2 Private Mode and Enterprise Mode (IEEE 802.1X).
- Optimal dLAN security with a 128-bit AES encryption.

- Remote management via the devolo dLAN AVpro manager software.
- Simple configuration via web interface.
- Optimal modification of the device for any usage scenario through network ports that can be disabled and the deactivation of the function buttons on the device.
- WLAN time control with configurable usage times.
- Two internal WLAN antennas; MIMO technology for the best transmission and reception performance.

2.5 Sample applications

2.5.1 dLAN pro 500 Wireless+ as a WLAN access point

By default, the dLAN pro 500 Wireless+ is configured as a WLAN access point and makes the dLAN pro network connected via the mains outlet available wirelessly to other client devices, such as laptops, IP radios or IP telephones. This is particularly practical if not all client stations are within range of a WLAN access point, for example because concrete walls disrupt the signal. With dLAN various rooms can be easily connected via the mains supply. And using the dLAN pro 500 Wireless+, every mains outlet can be turned quickly and easily into a WLAN connection with excellent reception quality.

The following illustration shows how the Internet connection is set up using the dLAN pro 500 Wireless+ and a router, and how the connection within the network is set up using additional dLAN pro devices.

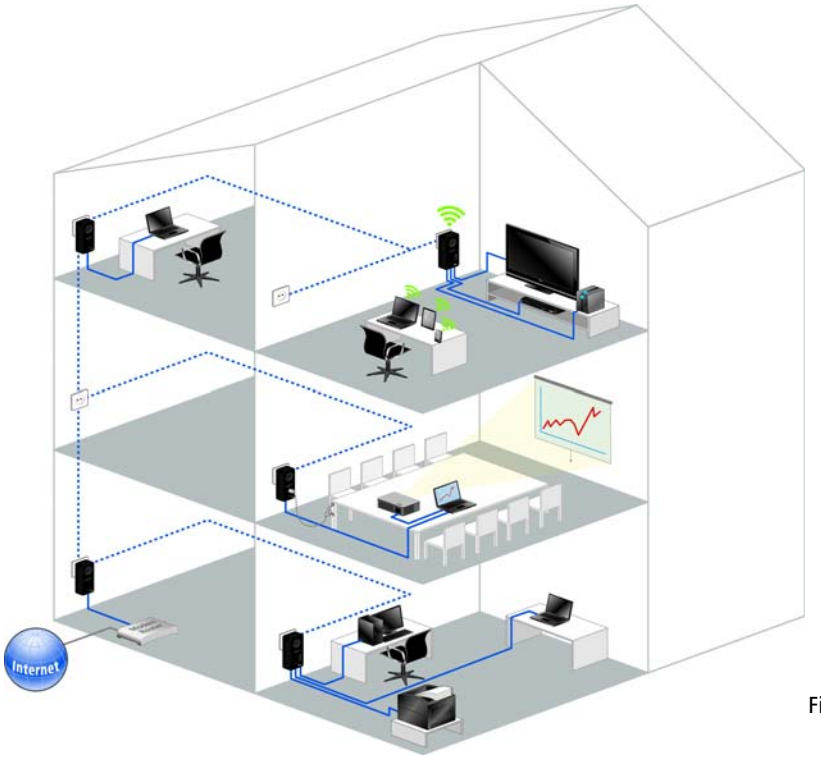


Fig. 1

2.5.2 dLAN pro 500 Wireless+ as a WLAN client

Alternatively, the dLAN pro 500 Wireless+ can also be configured as a WLAN client. In this case, the device connects the WLAN network with the devices in the dLAN pro network. This is especially practical if network access is not possible either via dLAN or via Ethernet wiring.

The following illustration describes how the dLAN pro 500 Wireless+ connects multiple computers in the dLAN pro network wirelessly using an existing router in another network, which, in turn, provides access to the Internet via Ethernet.

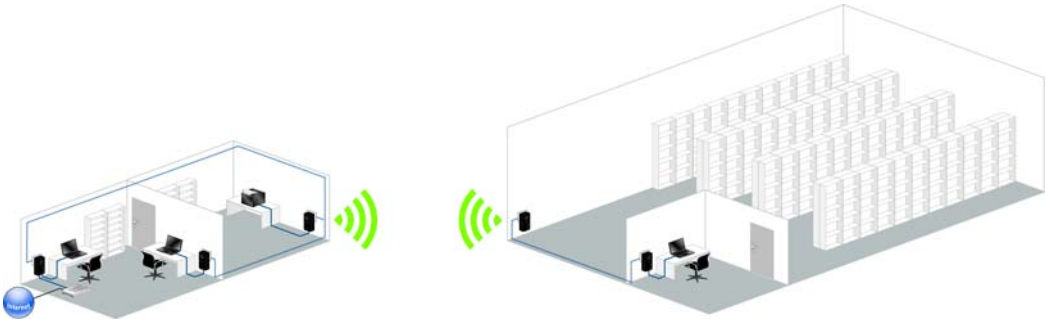


Fig. 2: Wi-Fi building connection

2.5.3 dLAN pro 500 Wireless+ and VLAN

Using the VLAN function, the dLAN pro 500 Wireless+ can establish more complex network architecture. The following illustration shows a building with **a single physical network architecture** that in turn has to be used by **two different companies separately and isolated**.

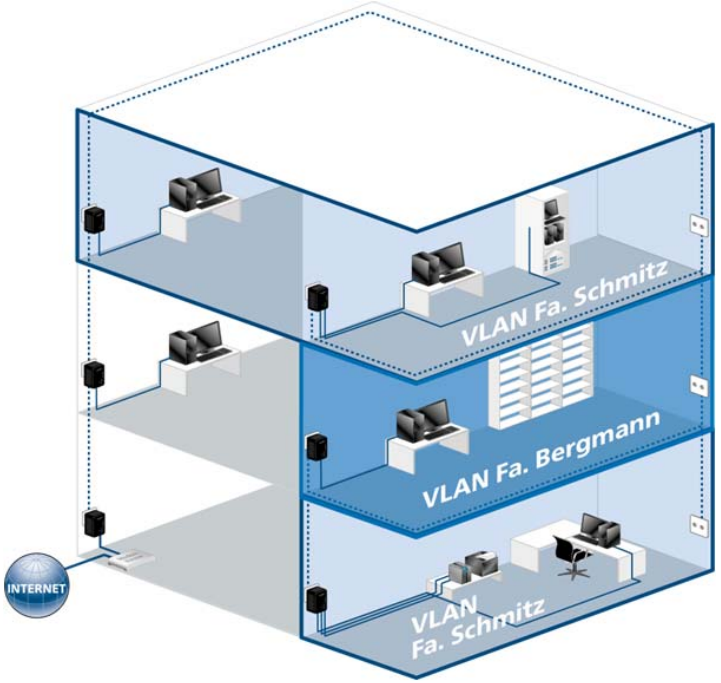


Fig. 3: Rented offices

All network-compatible devices are connected on a single dLAN pro network and share a broadband connection and a VLAN-capable router. All data traffic from each company in this building is contained in a separate VLAN. Here, each data packet sent over the dLAN pro network is given a VLAN tag specific to each dLAN pro 500 Wireless+.

Each VLAN tag contains a unique VLAN ID: The **VLAN of the Bergmann company**, for example, uses a **VLAN ID of "100"** while the **VLAN of the Schmitz company** uses a **VLAN ID of "200"**.

The dLAN pro 500 Wireless+ of the **Bergmann company only receives data packets** with the **VLAN ID of "100"**, and respectively, the dLAN pro 500 Wireless+ of the **Schmitz company** only receives **data packets** with the **VLAN ID of "200"**.

This configuration ensures that each company **has access only to its own assigned data traffic** even though all data runs through the same, commonly used physical network.

The advantages are obvious:

- The cost and burden of installing and operating multiple broadband access points are eliminated.
- The network infrastructure is quickly and easily reconfigured to match changes in room assignments.
- Complicated installation/uninstallation of network devices and the need to patch connections are eliminated.

You can find a detailed description for the VLAN configuration under **4.6 VLAN configuration**.

3 Initial use

This chapter covers everything you need to know to set up your dLAN pro 500 Wireless+. It will explain connecting the device and its functions. We will also briefly introduce the included devolo software.

Fig. 4 is country-specific

3.1 Package contents

Please ensure that the delivery is complete before beginning with the installation of your dLAN pro 500 Wireless+.

- **Single Kit**:
  - dLAN pro 500 Wireless+
  - Hard copy of installation guide
  - CD containing software and online documentation

or

- **Starter Kit**:
  - dLAN pro 500 Wireless+
  - dLAN 500 AVpro+
  - Network cable
  - Hard copy of installation guide
  - CD containing software and online documentation

devolo AG reserves the right to change the package contents without prior notice.

3.2 System requirements

- **All operating systems with network support**
- **dLAN AVpro manager**: Windows XP SP3 (32), Windows Vista Business SP2 (32/64), Windows 7 Professional SP1 (32/64), Windows 8 Pro (32/64), Ubuntu 12.04 LTS "Precise Pangolin" (32/64), Ubuntu 13.04 "Raring Ringtail" (32/64), OpenSuse 12.3 (32/64)
- **Network connection**

Please note that your computer or other device must feature a network adapter / network device with a network port.

To set up a dLAN pro network, you need at least two dLAN (AV)pro devices (200 Mbps or 500 Mbps).

3.3 Functions

The dLAN pro 500 Wireless+ has the following elements:

3.3.1 Control lamps

The indicator lights (LEDs) show all of the statuses for the dLAN pro 500 Wireless+ by illuminating and/or flashing in different ways:

Power

- **Green** flashing and illumination behaviour:
  - The LED lights up green when the dLAN pro 500 Wireless+ is operational.
  - The LED **flashes briefly**, if the dLAN pro 500 Wireless+ is in **PowerSave mode**.
  - The LED **flashes** at **quick, regular intervals**, if the dLAN pro 500 Wireless+ is connecting to the dLAN network (**pairing**).

dLAN

- **Off:** The LED does **not** light up. There is no connection to the dLAN pro network.

Check whether the device is connected to the mains supply correctly and whether the encryption process has been carried out successfully. For more information, refer to **3.4 Connecting the dLAN pro 500 Wireless+** *and* **5 dLAN pro network**.

- **Green**: The network connection is suitable for HD video streaming; flashes when data is being transmitted.
- **Orange**: The network connection is suitable for SD video streaming and online gaming; flashes when data is being transmitted.
- **Red**: The network connection is suitable for simple data transfer and Internet access; flashes when data is being transmitted.

Wi-Fi

- **Off:** The LED does **not** light up. The Wi-Fi connection is disabled.
- **Green** flashing and illumination behaviour:
  - The LED lights up when connected to the Wi-Fi network at **2.4 GHz**.
  - The LED **flashes** at **quick, regular intervals** when data is being transmitted.
  - The LED **flashes briefly** during WPS pairing.
- **Blue** flashing and illumination behaviour
  - The LED lights up when connected to the Wi-Fi network at **5 GHz**.
  - The LED **flashes** at **quick, regular intervals** when data is being transmitted.
  - The LED **flashes briefly** during WPS pairing.

Ethernet

- **Off:** The LED does **not** light up.

Check all of the cable connections and check if the connected network components are disabled.

- **Green**: The LED lights up when a connection to the Ethernet network exists; flashes when data is being transmitted.

3.3.2 Buttons

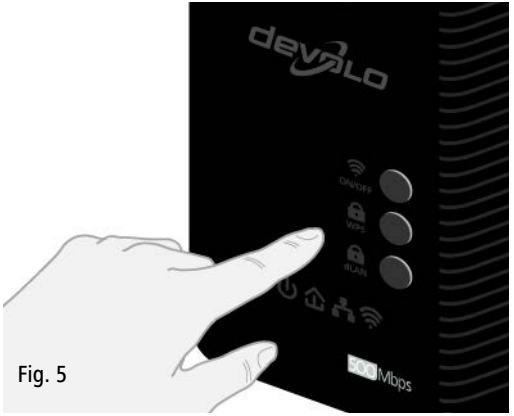


Fig. 5

All buttons can be enabled or disabled on the configuration interface.

ON/OFF

Use the ON/OFF button to switch the **Wi-Fi** function on or off.

Make sure that the Wi-Fi function in the factory defaults is enabled and the Wi-Fi encryption is set to WPA/WPA2 Private Mode. The default Wi-Fi key is the security ID of the dLAN pro 500 Wireless+. You will find the 16-character security ID on the label on the back of the housing.

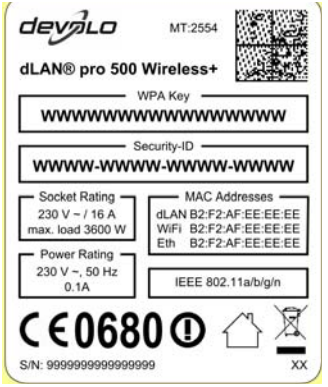


Fig. 6

WPS

With the WPS (**W**i-Fi **P**rotected **S**etup) encryption button, you secure your Wi-Fi network at the touch of a button.

WPS is one of the encryption standards developed by the Wi-Fi Alliance for increasing security in a Wi-Fi home network. The objective of WPS is to make it easier to add devices to an existing network. For more detailed information, refer to chapter **4.5.8 Wi-Fi Protected Setup (WPS)**.

dLAN

Via the dLAN encryption button, you secure your dLAN pro network at the touch of a button:

- To encrypt your dLAN pro network individually, press **each encryption button** on the connected devices for approx. **1 second** – within 2 minutes.
- To remove a dLAN pro device from your network, press the **encryption button** on the corresponding device **for at least 10 seconds**.

Reset

The **Reset** button (on the side of the housing) has two different functions:

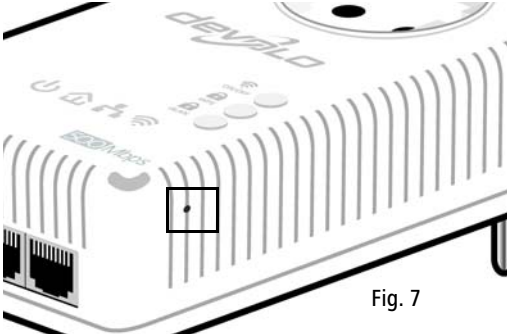


Fig. 7

- **The device restarts** if you press the Reset button **for less than 10 seconds**.
- To change the configuration of the dLAN pro 500 Wireless+ back to the **factory defaults**, press the Reset button **for more than 10 seconds**. Keep in mind that all settings that have already been configured will be lost!

The reset button can be pressed using the tip of a ball-point pen.

3.3.3 Network jacks

The three LAN ports can be used to connect computers or other network devices to the dLAN pro 500 Wireless+ via commercially available network cables.

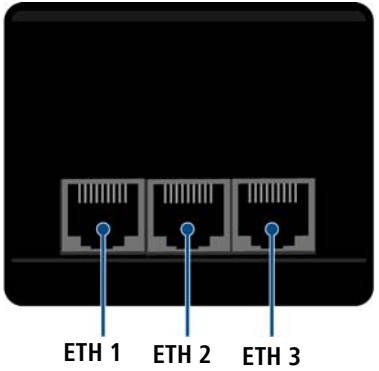


Fig. 8

3.3.4 Wi-Fi antennas

The internal Wi-Fi antennas are for connecting to other network devices wirelessly.

3.4 Connecting the dLAN pro 500 Wireless+

This section describes how to connect your dLAN pro 500 Wireless+ to a computer or other network device.

① Use a network cable to connect the dLAN pro 500 Wireless+ to the network port of your running computer or other network device.

② Plug the dLAN pro 500 Wireless+ into a wall socket.

The power outlet should be in range of the connected network device.
The dLAN pro 500 Wireless+ and the network device should be easily accessible.
To switch off the dLAN pro 500 Wireless+ or disconnect it from the mains supply, pull the mains plug out of the power outlet.

③ A dLAN pro network is set up as soon as at least one other dLAN pro device has been connected and plugged into the mains supply. You can use

dLAN AVpro manager, the encryption button **or** enter the dLAN password on the configuration interface to secure your dLAN pro network from unauthorised access. For information on how to proceed, please read further in chapter **4.4 Device configuration** and/or chapter **5 dLAN pro network**.

For detailed information about connecting other devolo dLAN devices, visit our website: www.devolo.com.

④ In order to be able to configure the **Wi-Fi network**, first install the configuration software as described in the following chapter.

3.4.1 Software for Windows and Linux

The dLAN AVpro manager configuration software is installed using the installation wizard.

- In addition to the individual encryption of your dLAN pro network, **devolo dLAN AVpro manager** offers other expanded dLAN functions.
- Via the **configuration interface** you can configure your Wi-Fi network (along with other actions).

To install the software, insert the included CD-ROM in the CD drive of your computer and follow the installation instructions.

Then you will find the link to the configuration interface as well as the installed dLAN AVpro manager in the program group Start ▷ All Programs ▷ devolo.

4 Network configuration

The dLAN pro 500 Wireless+ has a built-in configuration interface that can be called up using a standard web browser. All settings for operating the device can be modified here.

4.1 Calling up the built-in configuration interface

You will arrive at the built-in online configuration interface of the dLAN pro 500 Wireless+ by using the dLAN AVpro manager program under **Start ⇨ All Programs ⇨ devolo ⇨ dLAN AVpro manager**. Under **Expert mode ⇨ Unused devices** or in the **Network view**, call up the context menu (right-click on the device) of the dLAN pro 500 Wireless+ and click the **Open configuration website** entry to select it.

Then the program determines the current IP address and starts the configuration in the web browser.

By default, you will come directly to the configuration interface. However, if a login password was set via the option **Device configuration ⇨ Device security**, *you have to enter this first. Read more about this under* **4.4.1 Device security**.

4.2 Menu description

All menu functions are described in the corresponding interface as well as in the associated chapter in the manual. The sequence of the description in the manual follows the structure of the menu.

Click **Save** to save the settings of the respective area of the configuration interface.

Click **Back** to leave the respective area of the configuration interface.

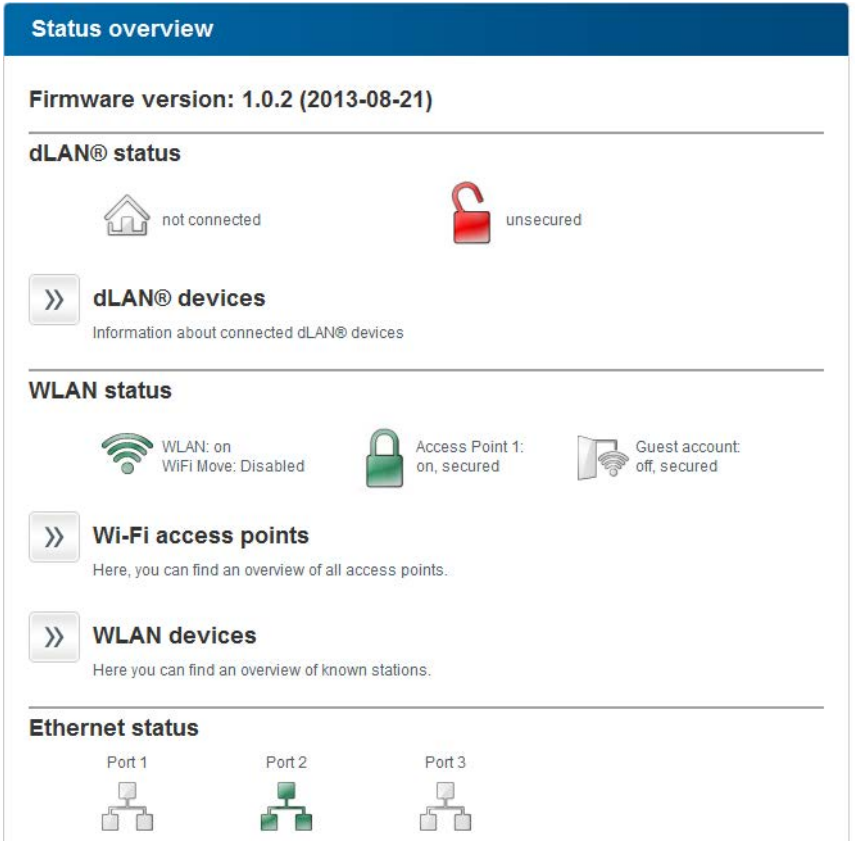
Select the desired language in the language selection list.

The five central areas of the configuration interface are displayed on the left edge. Click the button of an area to move directly into it.

- In the **Status overview** area, you get general information about all connected dLAN, Wi-Fi and LAN devices.
- You can make the various device settings for security, network, dLAN and time under **Device configuration**.
- You can modify Wi-Fi settings in the **WLAN configuration** area.
- You can make VLAN settings in the **VLAN configuration** area.
- The **Management** section is for resetting, securing and restoring your individual configurations. In addition, you can update the firmware of your dLAN pro 500 Wireless+ here.

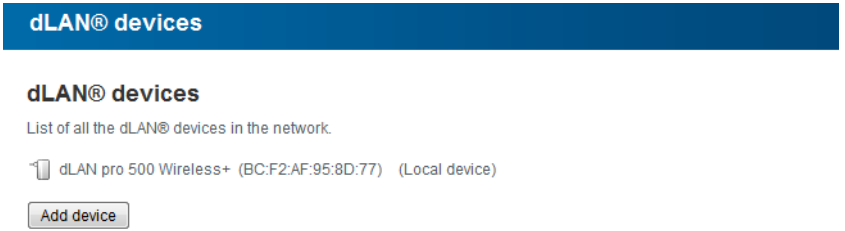
4.3 Status overview

In the **Status overview** area you can track the status of your connected dLAN, Wi-Fi and LAN devices.


Status overview
Firmware version: 1.0.2 (2013-08-21)
dLAN® status
not connected
unsecured
dLAN® devices
Information about connected dLAN® devices
WLAN status
WLAN: on
WiFi Move: Disabled
Access Point 1:
on, secured
Guest account:
off, secured
Wi-Fi access points
Here, you can find an overview of all access points.
WLAN devices
Here you can find an overview of known stations.
Ethernet status
Port 1
Port 2
Port 3

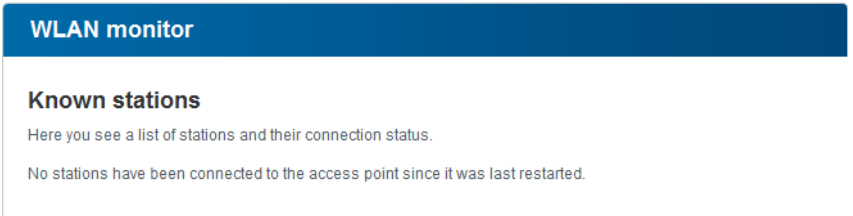
4.3.1 dLAN status

To display all connected dLAN devices, click either the **Ready to operate** icon or the **dLAN devices** arrow. Each connected dLAN device, regardless of whether it is connected locally or remote in the network, is displayed with its MAC address. Clicking the **lock** icon brings you directly to the **dLAN settings** (see **4.4.3 dLAN settings**).


dLAN® devices
dLAN® devices
List of all the dLAN® devices in the network.
dLAN pro 500 Wireless+ (BC:F2:AF:95:8D:77) (Local device)
Add device

4.3.2 WLAN status

To display all connected Wi-Fi devices, click either the **Ready to operate** icon or the **WLAN devices** arrow. Each connected Wi-Fi client is displayed with its MAC address.

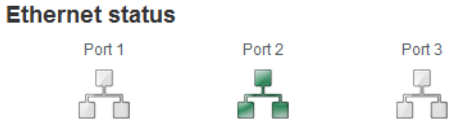

WLAN monitor
Known stations
Here you see a list of stations and their connection status.
No stations have been connected to the access point since it was last restarted.

Clicking the **Wi-Fi** icon brings you directly to the **WLAN configuration** area (see **4.5 WLAN configuration**), where you can configure settings for Wi-Fi network security. All access points that you have configured are listed under **Wi-Fi access points**.

If WLAN client mode is enabled, the display of the Wi-Fi access points is removed from the status overview.

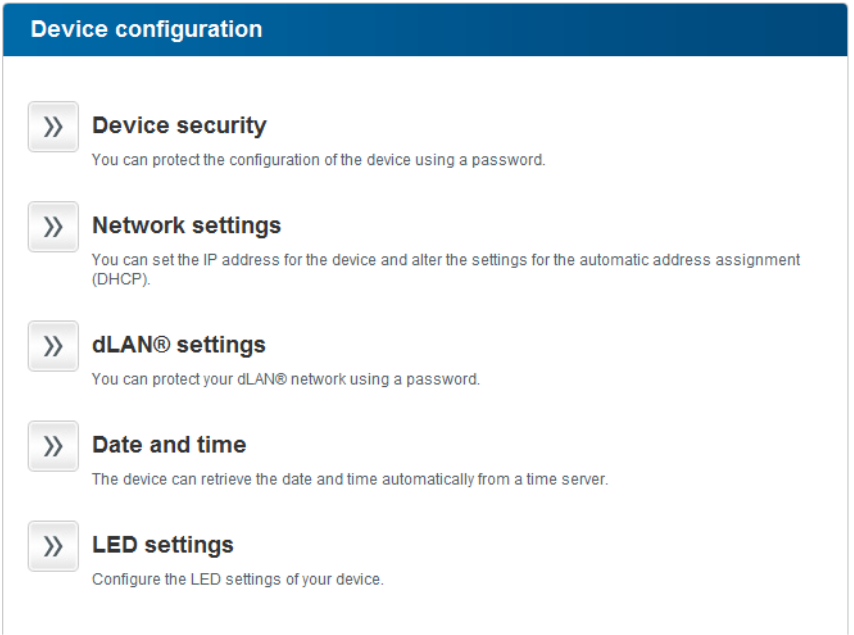
4.3.3 Ethernet status

The status and connection speed for the three network jacks are shown in this area.



4.4 Device configuration

In the configuration area of the device you can modify settings for security, network, dLAN, date and time as well as LED settings.


Device configuration
Device security
You can protect the configuration of the device using a password.
Network settings
You can set the IP address for the device and alter the settings for the automatic address assignment (DHCP).
dLAN® settings
You can protect your dLAN® network using a password.
Date and time
The device can retrieve the date and time automatically from a time server.
LED settings
Configure the LED settings of your device.

4.4.1 Device security

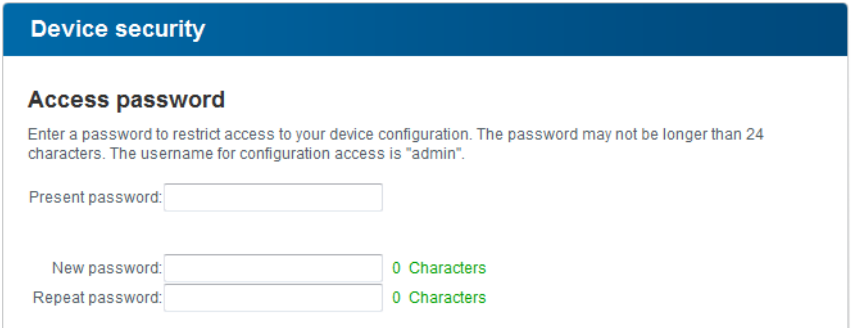
In this area you can control the access to the configuration interface as well as enable and disable the functions of the interfaces and buttons on the dLAN pro 500 Wireless+.

Password

You can set a login password for access to the configuration interface.

By default, the built-in configuration interface of the dLAN pro 500 Wireless+ is not protected with a password. However, we recommend assigning a password when the installation of the dLAN pro 500 Wireless+ is complete to protect it against tampering by third parties.

① To do so, first enter (if present) the current password and then enter the desired new password twice. Now the configuration interface is protected against unauthorised access with your individual password!


Device security
Access password
Enter a password to restrict access to your device configuration. The password may not be longer than 24 characters. The username for configuration access is "admin".
Present password:
New password:
0 Characters
Repeat password:
0 Characters

② Call up the configuration interface again later; the following window appears first:

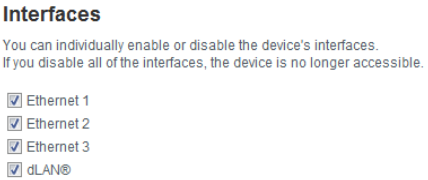
Windows Security
The server 169.254.21.210 at . requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
admin
Remember my credentials
OK
Cancel

③ Enter **admin** in the **User name** field and your individual password in the **Password** field.

The* admin *user name cannot be changed.

Interfaces

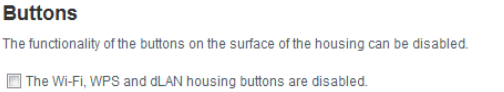
You can enable or disable the interface on the dLAN pro 500 Wireless+ by enabling or disabling the corresponding options.


Interfaces
You can individually enable or disable the device's interfaces.
If you disable all of the interfaces, the device is no longer accessible.
Ethernet 1
Ethernet 2
Ethernet 3
dLAN®

Note that the dLAN pro 500 Wireless+ can no longer be reached once all interfaces have been switched off.

Buttons

You can enable and disable the **Wi-Fi**, **WPS** and **dLAN encryption** functions on the dLAN pro 500 Wireless+ by enabling or disabling the option **The Wi-Fi, WPS and dLAN housing buttons are disabled**.


Buttons
The functionality of the buttons on the surface of the housing can be disabled.
The Wi-Fi, WPS and dLAN housing buttons are disabled.

Configuration over the web

The option **The device can be configured via the web** has to be enabled in order for the configuration interface to be accessible at all.

Configuration over the web
Configuration over the web interface can be disabled
The device can be configured over the web

Disabling this option rules out the possibility of configuring and thus accessing the interface. This status can be reversed only by resetting the device to the factory defaults (see the* Reset *section).

4.4.2 Network settings

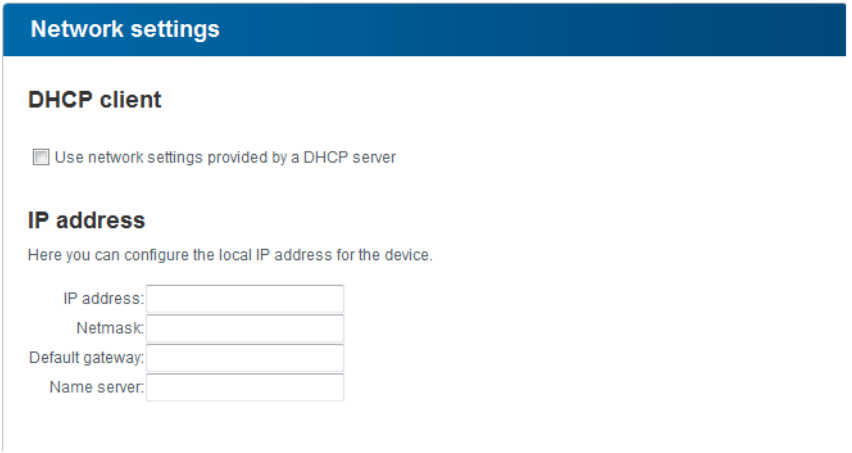
The dLAN pro 500 Wireless+ also communicates via the TCP/IP protocol as a component of your home network. The IP address required for this can either be entered manually as a static address or obtained **automatically** from a **DHCP server**.

The option **Use network settings provided by a DHCP server** is enabled in the factory defaults.

If a DHCP server is already present in the network for giving out IP addresses, have the option **Use network settings provided by a DHCP server** enabled so that the dLAN pro 500 Wireless+ automatically receives an address from it.

You can also assign a static IP address by specifying an **IP address**, **subnet mask**, **prefix length**, **name server** and **default gateway**.

If you ever forget the IP address of your dLAN pro 500 Wireless+, open the **dLAN AVpro manager** *to find the device in the network. Proceed as described under* **4.1 Calling up the built-in configuration interface**.

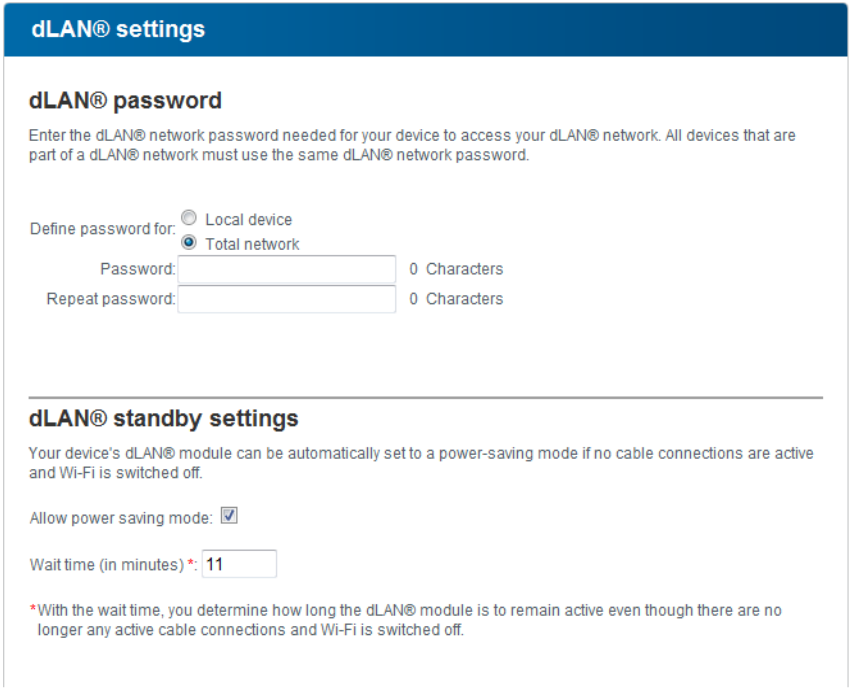


4.4.3 dLAN settings

In a dLAN pro network, all connected components must use the same password. The dLAN password can be defined using **dLAN AVpro manager**, via the **dLAN encryption button** (see chapter **5 dLAN pro network**) or in the **4.4.3 dLAN settings** section on the configuration interface.

When selecting the procedure, keep in mind the following:

- If the dLAN password is set using **dLAN AVpro manager** or via the **dLAN encryption button**, you can disregard the dLAN settings on the configuration interface, since the password is automatically forwarded.
- If the dLAN password is set or changed on the configuration interface, the password in **dLAN AVpro manager has to be adjusted** accordingly. The password is not forwarded automatically.


dLAN® settings
dLAN® password
Enter the dLAN® network password needed for your device to access your dLAN® network. All devices that are part of a dLAN® network must use the same dLAN® network password.
Define password for:
Local device
Total network
Password:
0 Characters
Repeat password:
0 Characters
dLAN® standby settings
Your device's dLAN® module can be automatically set to a power-saving mode if no cable connections are active and Wi-Fi is switched off.
Allow power saving mode:
Wait time (in minutes) *:
11
*With the wait time, you determine how long the dLAN® module is to remain active even though there are no longer any active cable connections and Wi-Fi is switched off.

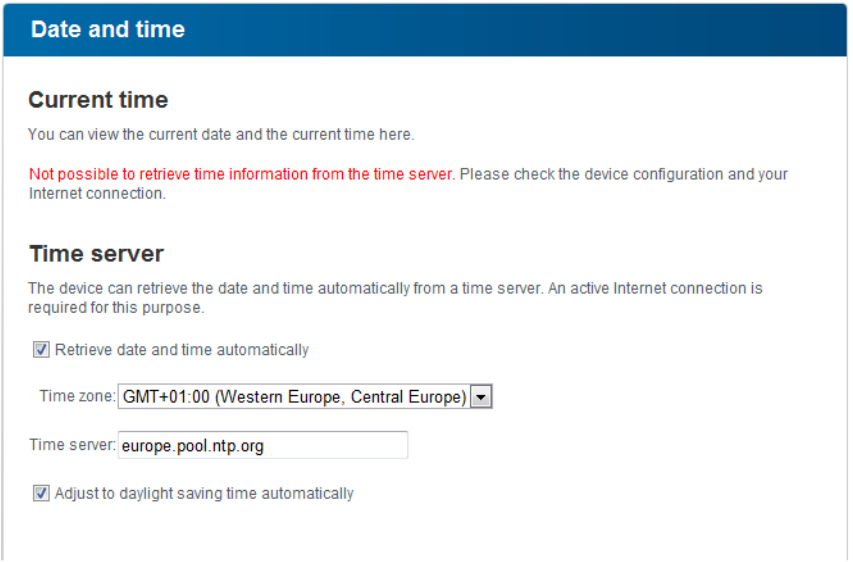
Activate the **Allow power saving mode** option, and enter a desired **wait time (in minutes)** for when the dLAN pro 500 Wireless+ should automatically change into save energy status.

4.4.4 Time server

A time server is a server on the Internet whose task consists of providing the exact time.

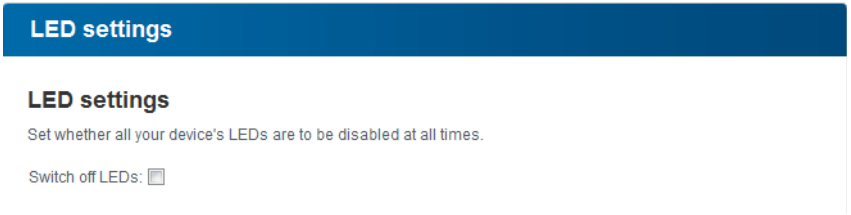
To see which Internet time server your computer uses to communicate, simply click the clock in the lower right corner of the screen and select the **Internet time** *tab.*

Enable the option **Retrieve date and time automatically**, so that the dLAN pro 500 Wireless+ can automatically synchronise the date and time. Select your **Time zone** and the **Time server**. If you have enabled the option **Adjust to daylight saving time automatically**, the dLAN pro 500 Wireless+ automatically adjusts to daylight saving time.


Date and time
Current time
You can view the current date and the current time here.
Not possible to retrieve time information from the time server. Please check the device configuration and your Internet connection.
Time server
The device can retrieve the date and time automatically from a time server. An active Internet connection is required for this purpose.
Retrieve date and time automatically
Time zone:
GMT+01:00 (Western Europe, Central Europe)
Time server:
europe.pool.ntp.org
Adjust to daylight saving time automatically

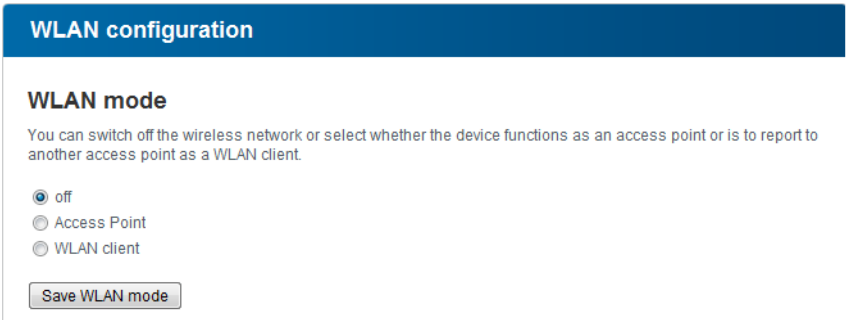
4.4.5 LED settings

Activate the **Switch off LEDs** option if they are intended to be switched off.



4.5 WLAN configuration

You can make all necessary Wi-Fi settings in the **Wi-Fi configuration** area. The device features three different modes: **Off**, **Access point** and **WLAN client**. Depending on the selection, the corresponding Wi-Fi functions and options are displayed.


WLAN configuration
WLAN mode
You can switch off the wireless network or select whether the device functions as an access point or is to report to another access point as a WLAN client.
off
Access Point
WLAN client
Save WLAN mode

WLAN configuration off

If you would like, you can completely shut off the Wi-Fi part of your dLAN pro 500 Wireless+, e.g. if you want to operate it exclusively as a simple dLAN device via the built-in Ethernet connections. To do so, under **WLAN configuration** select the **Off** mode and confirm your entry with **Save WLAN mode** or simply press the **Wi-Fi ON/OFF** button on the housing. The operating state of the device is displayed under **4.3 Status overview**.

Keep in mind that after saving this setting, you will be disconnected from any existing wireless connection to the dLAN pro 500 Wireless+. In this case, configure the device via Ethernet or dLAN.

WLAN configuration as access point

If you would like the dLAN pro 500 Wireless+ to act as an access point, select **Access point** mode under **WLAN configuration** and confirm your entry with **Save WLAN mode** or simply press the **Wi-Fi ON/OFF** button on the housing. The dLAN pro 500 Wireless+ automatically changes to Access point mode. The operating state of the device is displayed under **4.3 Status overview**.

WLAN configuration as client

If you would like the dLAN pro 500 Wireless+ to act as client, select **WLAN client** mode under **WLAN configuration** and confirm your entry with **Save WLAN mode**. The operating state of the device is displayed under **4.3 Status overview**.

If you select* WLAN client *mode,* WiFi Move Technology *is automatically disabled (also see* 4.5.5 WiFi Move Technology*).

4.5.1 Basic settings

In the **WLAN settings**, you can set the frequency band, time control, radius server and the parental settings, regardless of whether the dLAN pro 500 Wireless+ is set as an **Access point** or **WLAN client**. **The settings apply to both modes**.

For Wi-Fi operation of the dLAN pro 500 Wireless+, a (transmission) channel must be specified in a particular frequency range:

WLAN settings
Basic settings
Please select the basic settings for your device.
Frequency band: 2.4 GHz 5 GHz Channel: Auto Use 40-MHz channels: **
Please check whether all wireless connected devices support 5 GHz operating mode before enabling it!
Note: In 2.4 GHz mode the WLAN LED is green, in 5 GHz mode it is blue.

- Thirteen channels are available at the **standard 2.4 GHz** frequency.
- If you select the higher **5 GHz** frequency range, it is important to ensure that all of your connected devices also support this frequency band. **From channel 52 onward** you go into the **radar range**. When **accessing the device for the first time**, a **radar detection phase** starts automatically, during which the dLAN pro 500 Wireless+ cannot be accessed.

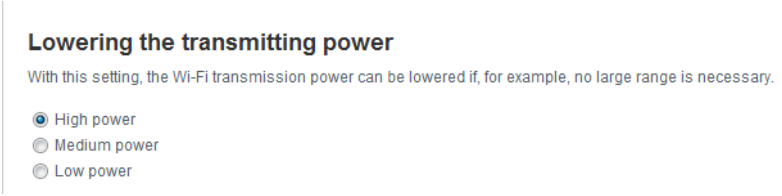
In both cases, we recommend keeping the default setting **Auto** since the dLAN pro 500 Wireless+ selects the channel regularly and independently in this setting. In other words, if the last connected station logs out, a search for a suitable channel is carried out immediately. If no stations are connected, the device automatically selects a channel every 15 minutes.

Pay attention to the various LED colours of the Wi-Fi LED. For more information, refer to chapter* 3.3.1 Control lamps*.

Keep the following in mind if you would like to use doubled channel width (*utilising 40 MHz channels*): The potential transfer rate is 300 Mbps instead of 150 Mbps when using wireless channels with doubled channel width, but increased interference can occur due to neighbouring access points.

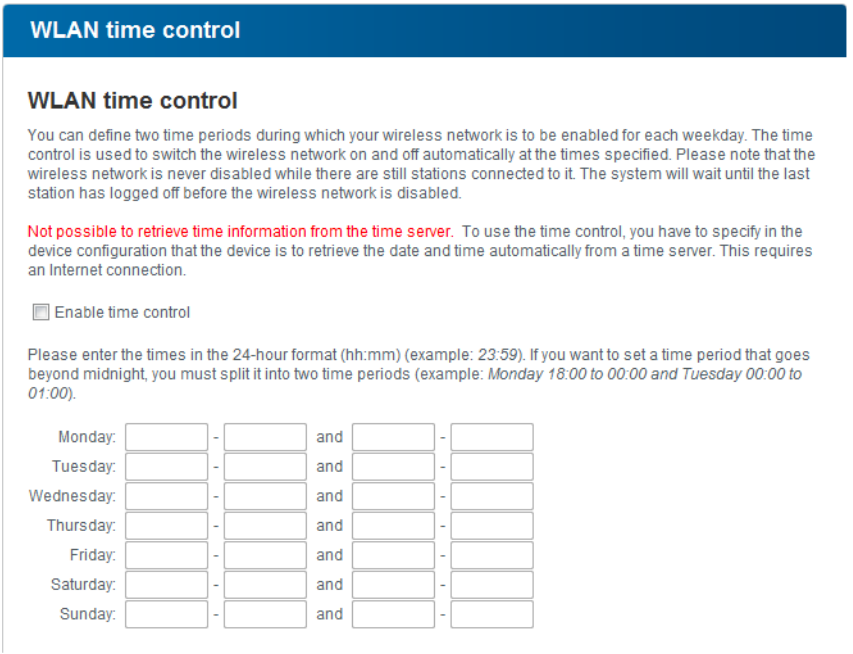
Lowering the transmitting power

In this section, you can adjust the Wi-Fi transmission level to your needs. I.e. if you do not require a large range. For example, if you are in the same room as the dLAN pro 500 Wireless+, select **low power**.


Lowering the transmitting power
With this setting, the Wi-Fi transmission power can be lowered if, for example, no large range is necessary.
High power
Medium power
Low power

4.5.2 WLAN time control

To be able to use the Wi-Fi time control, the option **Retrieve date and time automatically** must ***be enabled*** under **Device configuration ⇨ Date and time**. ***An enabled Internet connection is also required (see*** **4.4.4 Time server*)*.**


WLAN time control
WLAN time control
You can define two time periods during which your wireless network is to be enabled for each weekday. The time control is used to switch the wireless network on and off automatically at the times specified. Please note that the wireless network is never disabled while there are still stations connected to it. The system will wait until the last station has logged off before the wireless network is disabled.
Not possible to retrieve time information from the time server. To use the time control, you have to specify in the device configuration that the device is to retrieve the date and time automatically from a time server. This requires an Internet connection.
Enable time control
Please enter the times in the 24-hour format (hh:mm) (example: 23:59). If you want to set a time period that goes beyond midnight, you must split it into two time periods (example: Monday 18:00 to 00:00 and Tuesday 00:00 to 01:00).
Monday: - and -
Tuesday: - and -
Wednesday: - and -
Thursday: - and -
Friday: - and -
Saturday: - and -
Sunday: - and -

To be able to use the Wi-Fi time control, enable the option **Enable time control**. The time control automatically switches your wireless network on and off at certain times of the day.

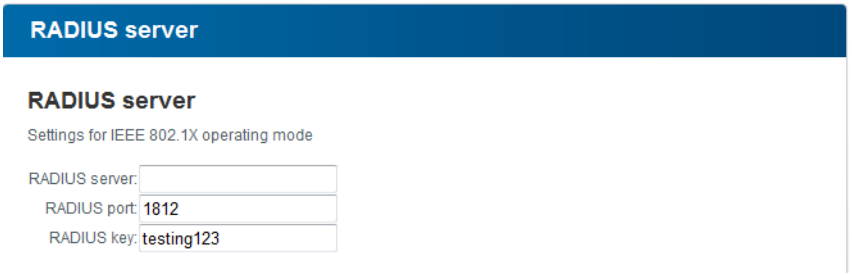
You can define two time periods during which your wireless network is to be enabled for each weekday. Then the time control automatically switches the wireless network on or off.

Keep in mind that, as long as the dLAN pro 500 Wireless+ registers connected stations, the wireless network remains enabled. The wireless network is not switched off until the last station has logged off.

4.5.3 RADIUS server

In addition to the **WPA/WPA2 Private Mode** encryption key, the dLAN pro 500 Wireless+ also supports **WPA/WPA2 Enterprise Mode (see 4.5.6 dLAN pro 500 Wireless+ as Access point** or **4.5.9 dLAN pro 500 Wireless+ as a WLAN client**). In addition to the **WLAN client** and the **access point**, there is also the **Radius server** in Enterprise Mode. As a central authentication server, it assumes the user administration for multiple access points.

If you would like to use a **RADIUS server**, assign a name, **Radius port** and **Radius key**.



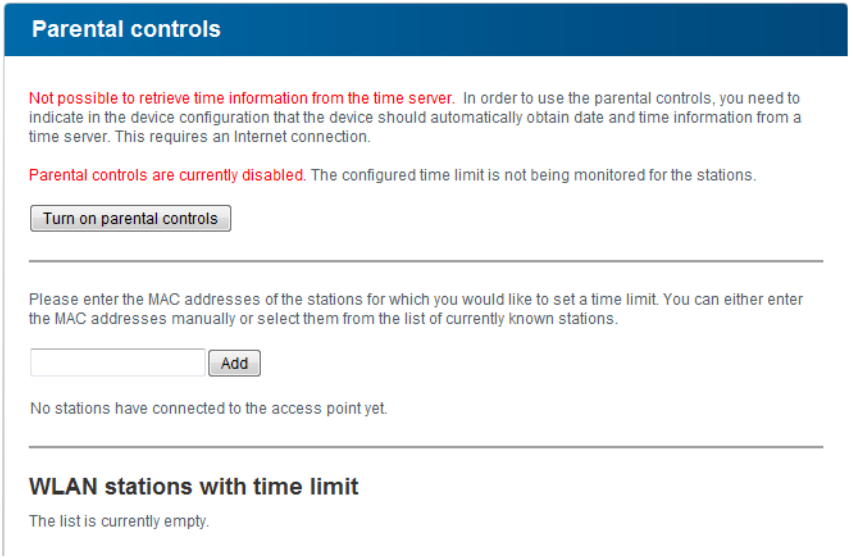
4.5.4 Parental controls

You can regulate Internet access for specific stations based on time using this function. For instance, to protect your children from excessive Internet use, you can define how long they may use the Internet per day.

Synchronisation with an Internet time server is necessary to be able to use the parental controls. In this case, the **time server** (**Device configuration ⇨ Date and time ⇨ Retrieve date and time automatically)** for the dLAN pro 500 Wireless+ has to be enabled and an enabled Internet connection is also re-

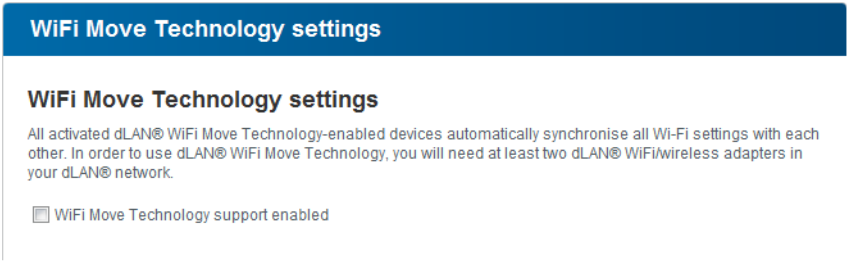
quired (see **4.4.4 Time server**). **The time server is enabled by default.**

If you would like to set up a daily time quota, enable the option **Turn on parental controls**. Now enter the MAC addresses for the stations for which you would like to set up a time quota. You can enter the MAC addresses manually or select them from the list of currently known stations (see **4.3.2 WLAN status ⇨ WLAN devices**). Confirm each entry with **Add**.


Parental controls
Not possible to retrieve time information from the time server. In order to use the parental controls, you need to indicate in the device configuration that the device should automatically obtain date and time information from a time server. This requires an Internet connection.
Parental controls are currently disabled. The configured time limit is not being monitored for the stations.
Turn on parental controls
Please enter the MAC addresses of the stations for which you would like to set a time limit. You can either enter the MAC addresses manually or select them from the list of currently known stations.
Add
No stations have connected to the access point yet.
WLAN stations with time limit
The list is currently empty.

4.5.5 WiFi Move Technology

Wi-Fi Move Technology is a function for synchronising the Wi-Fi settings of all **dLAN pro 500 Wireless+** connected to your network in the access Point mode.


WiFi Move Technology settings
WiFi Move Technology settings
All activated dLAN® WiFi Move Technology-enabled devices automatically synchronise all Wi-Fi settings with each other. In order to use dLAN® WiFi Move Technology, you will need at least two dLAN® WiFi/wireless adapters in your dLAN® network.
WiFi Move Technology support enabled

Observe the following rules when using WiFi Move Technology:

- When **Wi-Fi client mode** is enabled and **VLAN** is active, **WiFi Move Technology** remains disabled. To activate WiFi Move Technology, you must first switch off the VLAN function (see **4.6 VLAN configuration**) and select the Access point mode (see **4.5 WLAN configuration**).
- If you **switch on the VLAN function** (see **4.6 VLAN configuration**), **WiFi Move Technology is disabled automatically**.
- If you select **WLAN client mode** (see **4.5 WLAN configuration**), **WiFi Move Technology is disabled automatically.**

WiFi Move Technology support enabled

① Press the dLAN button of the dLAN pro 500 Wireless+ for which **the entire Wi-Fi configuration** is to be transferred to all other dLAN pro 500 Wireless+ devices.

② Then tap each dLAN button of the other dLAN pro 500 Wireless+ devices.

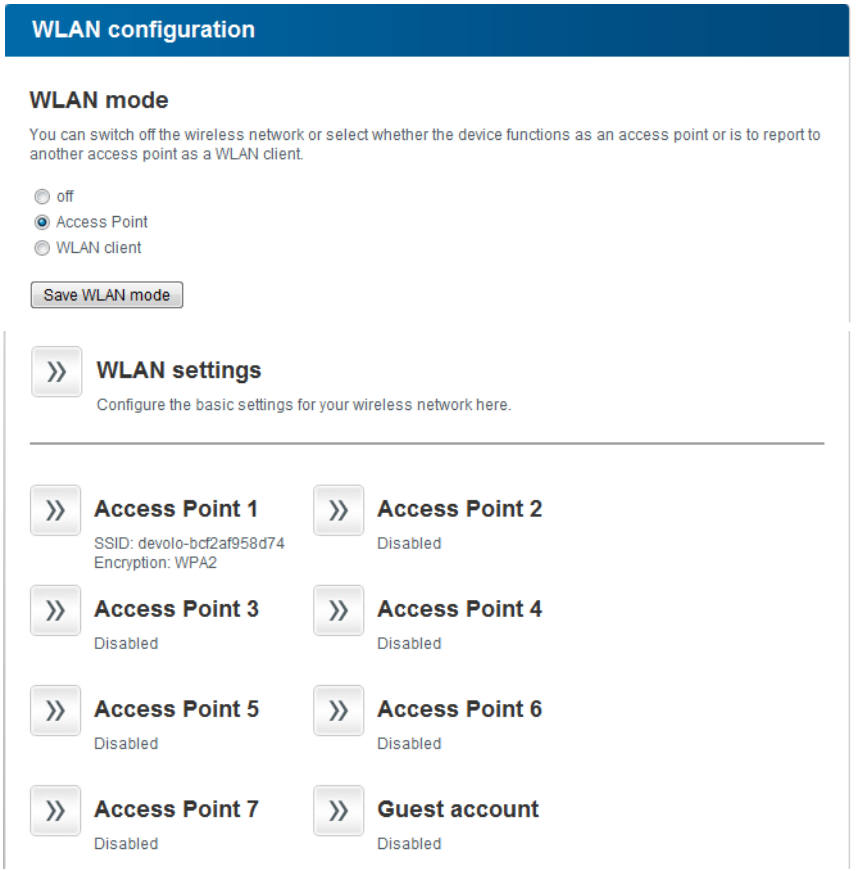
③ All dLAN pro 500 Wireless+ devices are now **continuously connected** to each other and, from now on, share changes to the **Wi-Fi configuration** with each other **automatically**.

Only* devolo dLAN pro devices *interchange Wi-Fi options.

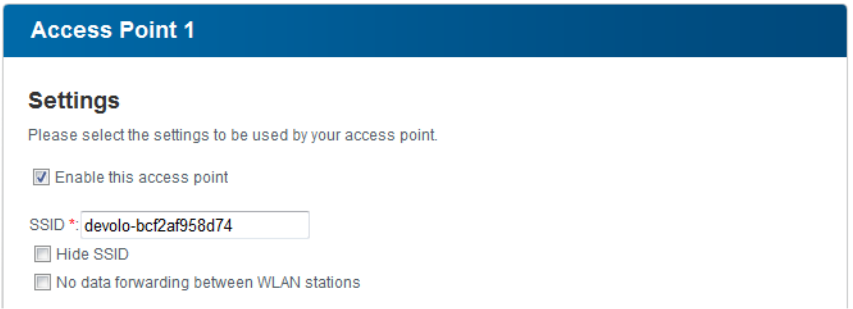
Wi-Fi configuration in factory defaults: In the factory default settings ***of the dLAN pro 500 Wireless+, the*** Wi-Fi function is enabled ***and the Wi-Fi encryption*** WPA/WPA2 Private Mode ***is configured. The default Wi-Fi key is the Wi-Fi key of the corresponding device. You will find the key on the label on the back of the housing.***

4.5.6 dLAN pro 500 Wireless+ as Access point

The dLAN pro 500 Wireless+ supports up to **7** access points (**multi-SSID**) **plus one guest account**, i.e. via the dLAN pro 500 Wireless+, you can operate up to **8 Wi-Fi networks**.


WLAN configuration
WLAN mode
You can switch off the wireless network or select whether the device functions as an access point or is to report to another access point as a WLAN client.
off
Access Point
WLAN client
Save WLAN mode
WLAN settings
Configure the basic settings for your wireless network here.
Access Point 1
SSID: devolo-bcf2af958d74
Encryption: WPA2
Access Point 2
Disabled
Access Point 3
Disabled
Access Point 4
Disabled
Access Point 5
Disabled
Access Point 6
Disabled
Access Point 7
Disabled
Guest account
Disabled

Settings for the access point


Access Point 1
Settings
Please select the settings to be used by your access point.
Enable this access point
SSID *: devolo-bcf2af958d74
Hide SSID
No data forwarding between WLAN stations

To enable a Wi-Fi network, select **Enable this access point**.

The **SSID** specifies the name of your wireless network. You can see this name when logging onto the Wi-Fi and thereby identify the correct subnet. If you enable the **Hide SSID** option, your wireless network name remains hidden. In this case, potential network users must know the exact SSID and enter it manually to be able to set up a connection.

A change to the SSID can interfere with all existing connections for a short time.

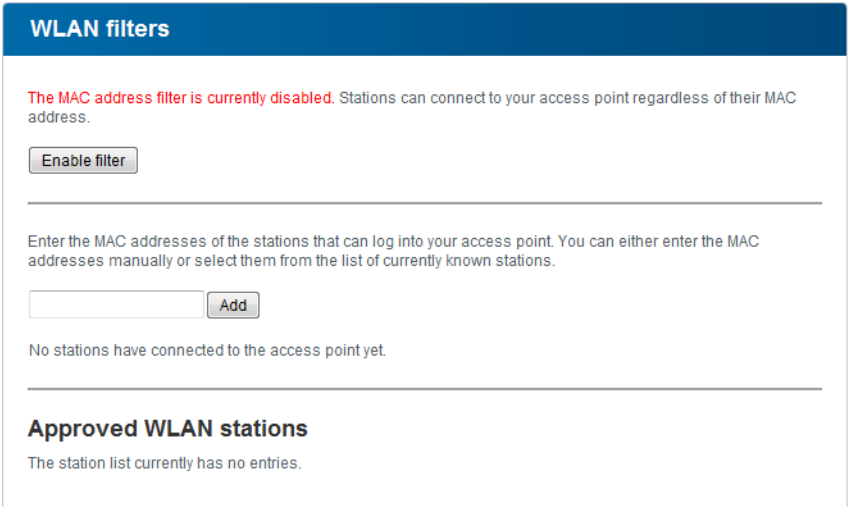
Some Wi-Fi clients have difficulty connecting to such hidden wireless networks. If the connection to a hidden SSID poses problems, first try to set up the connection with a visible SSID and only then try to hide it.

Depending upon the application scenario, security considerations may mean that it is to be forbidden for all devices to exchange data freely with each other. For this purpose, the option **No data forwarding between Wi-Fi stations** can be activated, which implements a genuine "peer-to-peer isolation"; all Wi-Fi devices configured as client are not able to exchange any data with each other, but only with the dLAN pro 500 Wireless+.

The factory defaults have this option disabled, i.e. all Wi-Fi devices present in the network can freely exchange data with each other ("peer-to-peer" mode).

WLAN filters

In addition to encryption, you can secure your wireless network even more by using a Wi-Fi filter to limit access via Wi-Fi to the dLAN pro 500 Wireless+ for selected devices. Even if the encryption is switched off, the device will not establish a connection.


WLAN filters
The MAC address filter is currently disabled. Stations can connect to your access point regardless of their MAC address.
Enable filter
Enter the MAC addresses of the stations that can log into your access point. You can either enter the MAC addresses manually or select them from the list of currently known stations.
Add
No stations have connected to the access point yet.
Approved WLAN stations
The station list currently has no entries.

The Wi-Fi filter should be used only as an additional option. By using it you could limit access to your wireless network, but without encryption it would be relatively easy for third parties to eavesdrop on all of your data transmissions.

To use the Wi-Fi filter, enable the option **Enable filters**. Now you can enter various network devices by means of what is known as your MAC address for access to your dLAN pro 500 Wireless+. Confirm each entry with **Add**. Network devices or stations connected to your dLAN pro 500 Wireless+ are automatically listed, that is, to enable an already connected station for the dLAN pro 500 Wireless+, simply select the MAC address of the respective device and confirm it with **Add**. This then appears under **Approved Wi-Fi stations**. To remove an enabled station, select its MAC address and confirm it with **Delete**.

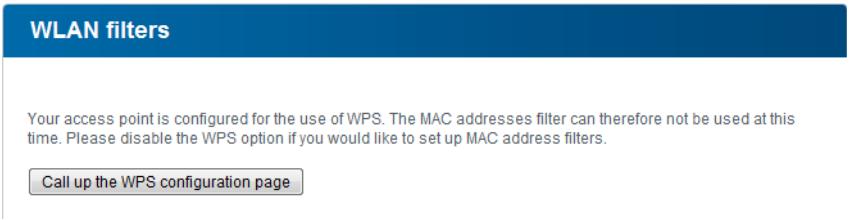
The MAC address designates the hardware interface of each individual network device uniquely (e.g. the Wi-Fi adapter of a computer or the Ethernet port of a printer). It consists of six double-digit hexadecimal numbers, each separated by a colon (e.g. 00:0B:3B:37:9D:C4). In general, the MAC address is on the housing of the device.

You can easily determine the MAC address of a Windows computer by opening the window with the command prompt under **Start** ▷ **All Programs** ▷ **Accessories** ▷ **Command Prompt**. Enter the command **IPCONFIG /ALL** here. The MAC address is displayed under the designation **Physical address**.

After entering the MAC addresses, do not forget to click the **Save** button. If the entered values are incorrect (e.g. because the colons are missing), a corresponding error message is displayed.

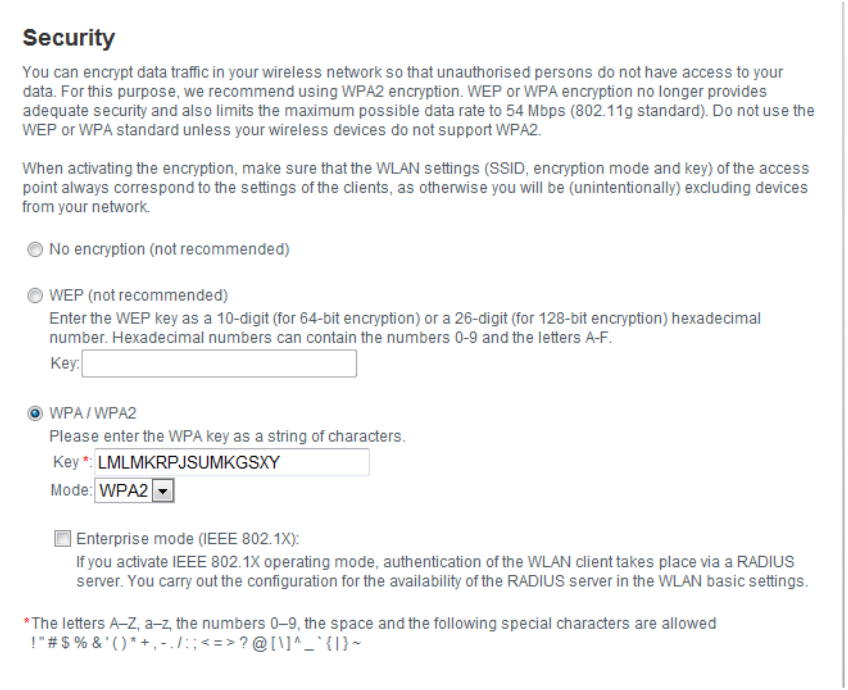
Keep in mind that you also have to enter the MAC address of your own computer if you are connected to the dLAN pro 500 Wireless+ not via the Ethernet port, but via Wi-Fi. Otherwise you will block your own access to the device via Wi-Fi by activating the Wi-Fi filter!

If you enabled WPS, the access restriction is disabled by a MAC filter (see **4.5.8 Wi-Fi Protected Setup (WPS)**).


WLAN filters
Your access point is configured for the use of WPS. The MAC addresses filter can therefore not be used at this time. Please disable the WPS option if you would like to set up MAC address filters.
Call up the WPS configuration page

Security (encryption)

Without encryption, not only are all data transmitted from client computers to the dLAN pro 500 Wireless+ in your wireless network without protection, but there is also no password prompt to establish the connection. If no other security measures were set up, such as a Wi-Fi filter (see **WLAN filters**), third parties can gain access to your network at any time and, for example, share your Internet connection. Usually this happens without you noticing it.


Security
You can encrypt data traffic in your wireless network so that unauthorised persons do not have access to your data. For this purpose, we recommend using WPA2 encryption. WEP or WPA encryption no longer provides adequate security and also limits the maximum possible data rate to 54 Mbps (802.11g standard). Do not use the WEP or WPA standard unless your wireless devices do not support WPA2.
When activating the encryption, make sure that the WLAN settings (SSID, encryption mode and key) of the access point always correspond to the settings of the clients, as otherwise you will be (unintentionally) excluding devices from your network.
No encryption (not recommended)
WEP (not recommended)
Enter the WEP key as a 10-digit (for 64-bit encryption) or a 26-digit (for 128-bit encryption) hexadecimal number. Hexadecimal numbers can contain the numbers 0-9 and the letters A-F.
Key:
WPA / WPA2
Please enter the WPA key as a string of characters.
Key *: LMLMKRPJSUMKGSXY
Mode: WPA2
Enterprise mode (IEEE 802.1X):
If you activate IEEE 802.1X operating mode, authentication of the WLAN client takes place via a RADIUS server. You carry out the configuration for the availability of the RADIUS server in the WLAN basic settings.
*The letters A–Z, a–z, the numbers 0–9, the space and the following special characters are allowed
! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

To secure the data transmission in your wireless network there are two security standards available for the Access Point mode.

- The older and weaker **WEP** standard can protect communication with the help of a key having either **10 or 26 hexadecimal characters**.

- The state-of-the-art **WPA/WPA2 (Wi-Fi Protected Access) Private Mode** methods allow individualised keys consisting of **letter and numbers and the displayed special characters with a length of up to 63 characters**. You can simply enter them via the keyboard. Under **Mode**, you can limit access of clients to the dLAN pro 500 Wireless+ to the method you have selected. In addition, the dLAN pro 500 Wireless+ also supports the **WPA/WPA2 Enterprise Mode** encryption key. As a central authentication server, the RADIUS server assumes the user administration (for multiple access points; **see 4.5.3 RADIUS server**).

Enterprise Mode does* not *support any WPS.

Save all modified settings before leaving this configuration area again.

The* factory defaults *have the dLAN pro 500 Wireless+ configured as an access point and the* WPA/WPA2 Private Mode *Wi-Fi encryption is set with the* security ID as the default Wi-Fi key. *You will find the 16-character security ID on the label on the back of the housing.

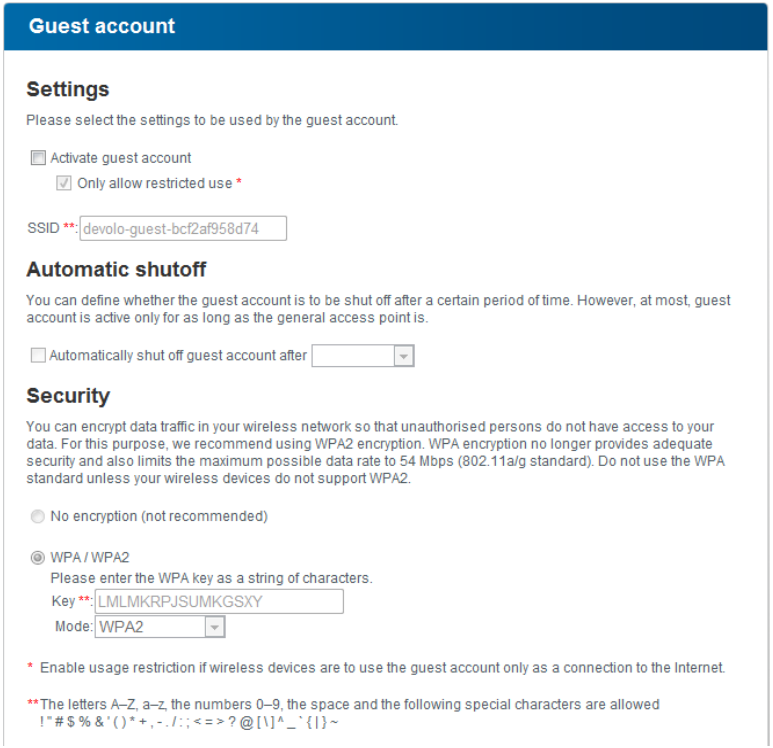
When activating the encryption, make sure that the Wi-Fi settings (SSID, encryption mode and encryption key) of the access point always correspond to the settings of the clients, as otherwise you will be (unintentionally) excluding devices from your network.

You should always encrypt the connections in your Wi-Fi. Otherwise anyone within range could penetrate into your home network and, for example, share your Internet connection. If possible, always select the better WPA/WPA2 encryption method. Only use WEP if one of your wireless terminal devices does not operate with a better standard.

4.5.7 Guest account

If you have friends or acquaintances visiting and you want to provide them with Internet access but without giving away the password for your Wi-Fi, you can set up a separate guest account in addition to the main In-

ternet connection. The guest account can have its own SSID, time limit and Wi-Fi password. This way your visitors can surf the Internet without having access to your local network.


Guest account
Settings
Please select the settings to be used by the guest account.
Activate guest account
Only allow restricted use *
SSID **: devolo-guest-bcf2af958d74
Automatic shutoff
You can define whether the guest account is to be shut off after a certain period of time. However, at most, guest account is active only for as long as the general access point is.
Automatically shut off guest account after
Security
You can encrypt data traffic in your wireless network so that unauthorised persons do not have access to your data. For this purpose, we recommend using WPA2 encryption. WPA encryption no longer provides adequate security and also limits the maximum possible data rate to 54 Mbps (802.11a/g standard). Do not use the WPA standard unless your wireless devices do not support WPA2.
No encryption (not recommended)
WPA / WPA2
Please enter the WPA key as a string of characters.
Key **: LMLMKRPJSUMKGSXY
Mode: WPA2
* Enable usage restriction if wireless devices are to use the guest account only as a connection to the Internet.
**The letters A–Z, a–z, the numbers 0–9, the space and the following special characters are allowed
! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

Settings

To set up a guest account, enable the **Activate guest account** option.

If you would like to restrict internet use, enable the **Only allow restricted use** option as well.

Define the name of the guest network in the **SSID** field.

Automatic shutoff

If you would like to set a time limit for the guest account, enable the option **Automatically shut off guest account after ...** and enter the desired time limit.

Note that the guest account depends on the Wi-Fi settings of the dLAN pro 500 Wireless+ and can only be enabled just as long.

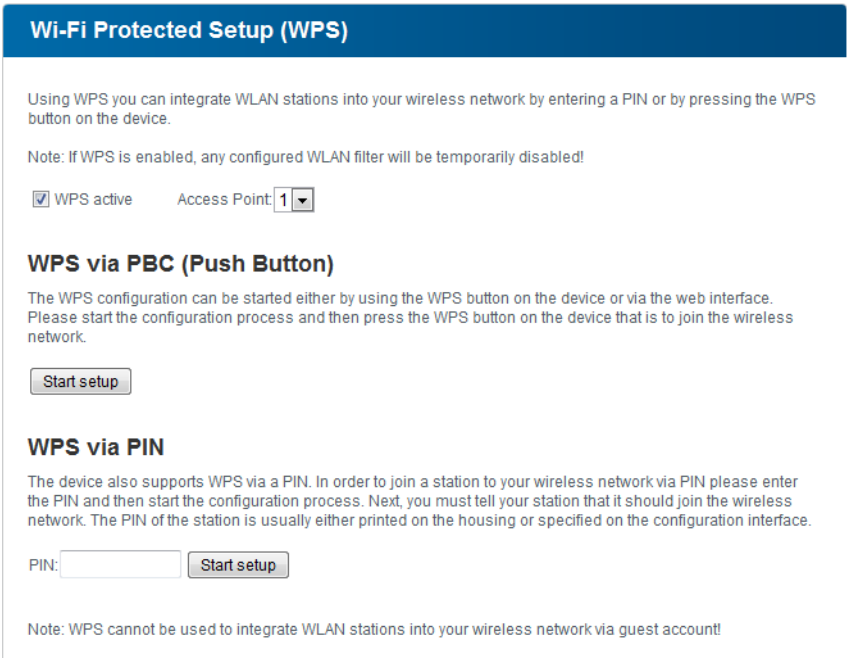
Security (encryption)

You should also encrypt the guest account to prevent anyone in signal range from intruding into your home network and sharing your Internet connection**.** **WPA/WPA2 (Wi-Fi Protected Access) Private Mode** security standards are available for this.

WPA/WPA2 (Wi-Fi Protected Access) allows individual keys consisting of **letters and numbers and the displayed special characters with a length of up to 63 characters**. You can simply enter this using the keyboard, without having to convert it into hexadecimal format first. Under **Mode**, you can limit access to the dLAN pro 500 Wireless+ to the method you have selected.

4.5.8 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) is one of the international encryption standards developed by the Wi-Fi Alliance for easily and quickly setting up a secure wireless network. The encryption keys of the respective Wi-Fi client are transmitted automatically and continuously to the other Wi-Fi client(s) of the wireless network. The dLAN pro 500 Wireless+ offers two different variants for transmitting these encryption keys:


Wi-Fi Protected Setup (WPS)
Using WPS you can integrate WLAN stations into your wireless network by entering a PIN or by pressing the WPS button on the device.
Note: If WPS is enabled, any configured WLAN filter will be temporarily disabled!
WPS active
Access Point: 1
WPS via PBC (Push Button)
The WPS configuration can be started either by using the WPS button on the device or via the web interface. Please start the configuration process and then press the WPS button on the device that is to join the wireless network.
Start setup
WPS via PIN
The device also supports WPS via a PIN. In order to join a station to your wireless network via PIN please enter the PIN and then start the configuration process. Next, you must tell your station that it should join the wireless network. The PIN of the station is usually either printed on the housing or specified on the configuration interface.
PIN:
Start setup
Note: WPS cannot be used to integrate WLAN stations into your wireless network via guest account!

WPS via PBC (Push Button Configuration):

① Start the encryption process on the dLAN pro 500 Wireless+

- ○ either by pressing the **WPS button** on the **front panel of the device** or
- ○ by pressing the **Start setup** button on the user interface under **Wi-Fi configuration** ▷ **Wi-Fi Protected Setup (WPS)**.

② Then press either the WPS key of the Wi-Fi client you are adding or the WPS button on the configuration interface. Now the devices exchange their encryption keys and establish a secure Wi-Fi connection. The Wi-Fi LED on the front panel indicates the synchronisation process by flashing.

WPS via PIN:

① To interconnect Wi-Fi clients securely in your wireless network via PIN variants, enter an individualised key in the configuration interface under **Wi-Fi configuration** ▷ **Wi-Fi Protected Setup (WPS)** ▷ **PIN** and start the encryption process by pressing the **Start setup** button.

② Open the configuration interface of the Wi-Fi client to be added and transmit the PIN selected on the dLAN pro 500 Wireless+. Confirm the encryption process as described there. Now the devices exchange their encryption keys and establish a secure Wi-Fi connection. The Wi-Fi LED on the front panel indicates the synchronisation process by flashing.

The client can also create the PIN; this must then be entered onto the configuration interface of the dLAN pro 500 Wireless+.

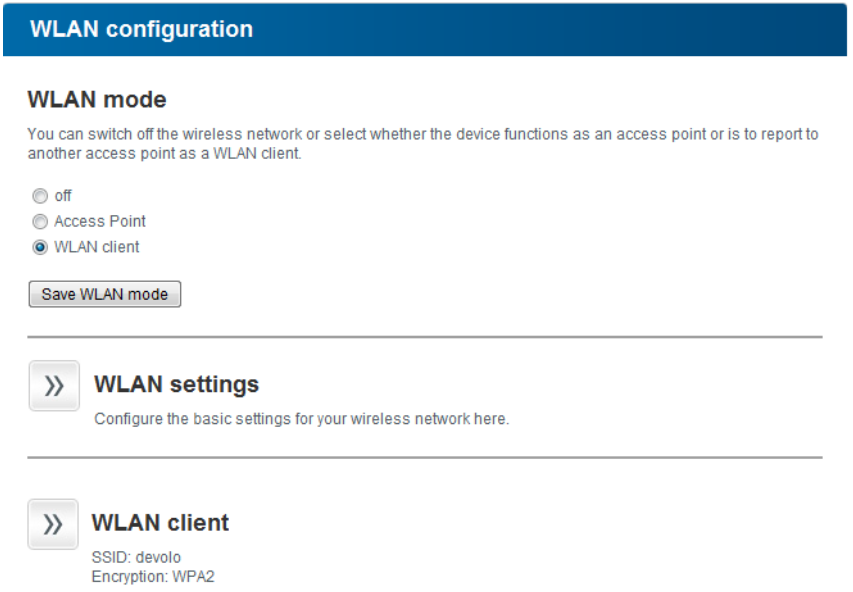
Use of the **WPS** process implies **WPA/WPA2 Private Mode**. For that reason, keep in mind the following automatic settings depending on the encryption standard (also refer to **4.4.1 Device security**), i.e.

- if under **Wi-Fi configuration** ▷ **Access Point No encryption** is selected in advance, **WPA/WPA2 Private Mode** is set automatically. The newly generated password is displayed under **Wi-Fi configuration** ▷ **Access Point** in the **Key** field.
- if under **Wi-Fi configuration** ▷ **Access Point WEP** is selected in advance, **WPA/WPA2 Private Mode** is set automatically. The newly generated password is displayed under **Wi-Fi configuration** ▷ **Access Point** in the **Key** field.
- if under **Wi-Fi configuration** ▷ **Access Point WPA/WPA2 Private Mode** is selected in

advance, this setting remains with the previously assigned password.

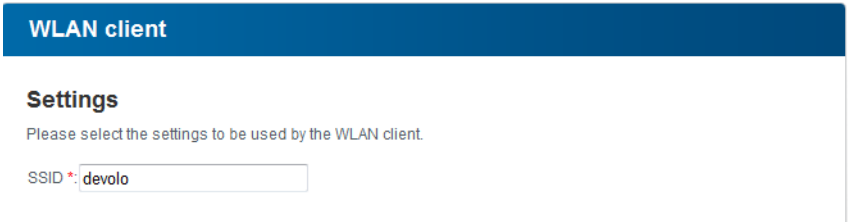
4.5.9 dLAN pro 500 Wireless+ as a WLAN client

If you have defined the dLAN pro 500 Wireless+ as a Wi-Fi client, the following menu appears:


WLAN configuration
WLAN mode
You can switch off the wireless network or select whether the device functions as an access point or is to report to another access point as a WLAN client.
off
Access Point
WLAN client
Save WLAN mode
WLAN settings
Configure the basic settings for your wireless network here.
WLAN client
SSID: devolo
Encryption: WPA2

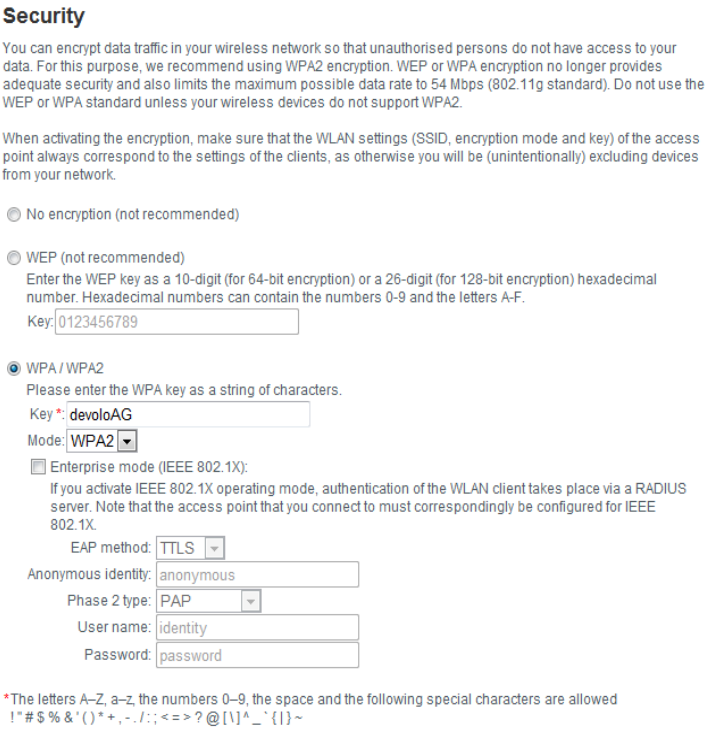
For a description of **WLAN settings**, *refer to chapter* **4.5.1 Basic settings**.

In the **SSID** field, enter the SSID of the access point for which you would like to register.



Security (encryption)

To secure the data transmission in your wireless network there are two security standards available for Wi-Fi Client mode.


Security
You can encrypt data traffic in your wireless network so that unauthorised persons do not have access to your data. For this purpose, we recommend using WPA2 encryption. WEP or WPA encryption no longer provides adequate security and also limits the maximum possible data rate to 54 Mbps (802.11g standard). Do not use the WEP or WPA standard unless your wireless devices do not support WPA2.
When activating the encryption, make sure that the WLAN settings (SSID, encryption mode and key) of the access point always correspond to the settings of the clients, as otherwise you will be (unintentionally) excluding devices from your network.
No encryption (not recommended)
WEP (not recommended)
Enter the WEP key as a 10-digit (for 64-bit encryption) or a 26-digit (for 128-bit encryption) hexadecimal number. Hexadecimal numbers can contain the numbers 0-9 and the letters A-F.
Key: 0123456789
WPA / WPA2
Please enter the WPA key as a string of characters.
Key *: devoloAG
Mode: WPA2
Enterprise mode (IEEE 802.1X):
If you activate IEEE 802.1X operating mode, authentication of the WLAN client takes place via a RADIUS server. Note that the access point that you connect to must correspondingly be configured for IEEE 802.1X.
EAP method: TTLS
Anonymous identity: anonymous
Phase 2 type: PAP
User name: identity
Password: password
*The letters A–Z, a–z, the numbers 0–9, the space and the following special characters are allowed
! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

- The older and weaker **WEP** standard can protect communication with the help of a key having either **10 or 26 hexadecimal characters**.
- The state-of-the-art **WPA/WPA2 (Wi-Fi Protected Access) Private Mode** methods allow individualised keys consisting of **letter and numbers and the displayed special characters with a length of up to 63 characters**. You can simply enter them via the keyboard. Under **Mode**, you can limit access of clients to the dLAN pro 500 Wireless+ to the method you have selected. In addition, the dLAN pro 500 Wireless+ also supports the **WPA/WPA2 Enterprise Mode** encryption key. As a central authentication server, the RADIUS server assumes the user administration (for multiple access points; **see chapter 4.5.3 RADIUS server**).

Enterprise Mode does* not *support any WPS.

Save all modified settings before leaving this configuration area again.

The* factory defaults *have the dLAN pro 500 Wireless+ configured as an access point and the* WPA/WPA2 Private Mode *Wi-Fi encryption is set with the* security ID as the default Wi-Fi key. *You will find the 16-character security ID on the label on the back of the housing.

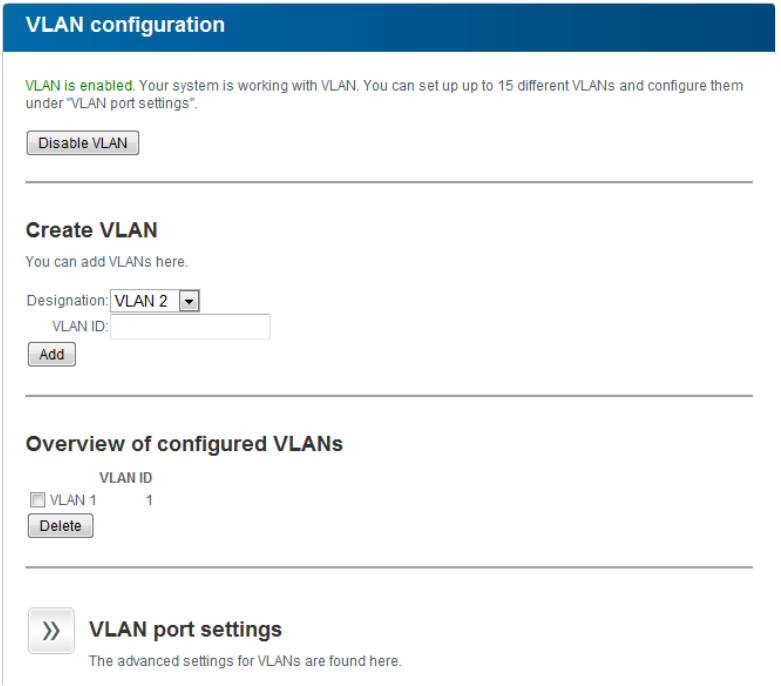
When activating the encryption, make sure that the Wi-Fi settings (SSID, encryption mode and encryption key) of the access point always correspond to the settings of the client, as otherwise you will be (unintentionally) excluding devices from your network.

4.6 VLAN configuration

you can select whether you would like to disable the VLAN configuration completely or use it. To do so, press the **Enable VLAN** or **Disable VLAN** button. If VLAN is disabled, all Ethernet ports, the dLAN port and the Wi-Fi access points are interconnected, i.e. in this operating mode the VLAN settings have no influence on the behaviour of the dLAN pro 500 Wireless+.

Observe the following rules when using the VLAN function:

- When **VLAN is active**, **WiFi Move Technology remains disabled**. To enable WiFi Move Technology, you must first switch off the VLAN function (see **4.5.5 WiFi Move Technology**).
- If you **enable the VLAN function** (see **4.5.5 WiFi Move Technology**), **WiFi Move Technology is disabled**.


VLAN configuration
VLAN is enabled. Your system is working with VLAN. You can set up up to 15 different VLANs and configure them under "VLAN port settings".
Disable VLAN
Create VLAN
You can add VLANs here.
Designation: VLAN 2
VLAN ID:
Add
Overview of configured VLANs
VLAN ID
VLAN 1 1
Delete
VLAN port settings
The advanced settings for VLANs are found here.

4.6.1 Create VLAN

The factory defaults have VLAN 1 configured with VLAN ID 2. You can configure additional VLANs under **Create VLAN**. In doing so, a VLAN (VLAN 1 to VLAN 15) has to be selected and a VLAN ID (1 to 4094) assigned. When creating VLANs, already assigned VLAN IDs cannot be assigned a second time. Configured VLANs are illustrated in the overview.

When configuring the VLANs and the VLAN port settings, the configuration interface of the dLAN pro 500 Wireless+ should remain accessible, i.e. configurable. If you ever "lock" yourself out in spite of this, the device has to be returned to the factory defaults by being reset (see the* Reset *section).

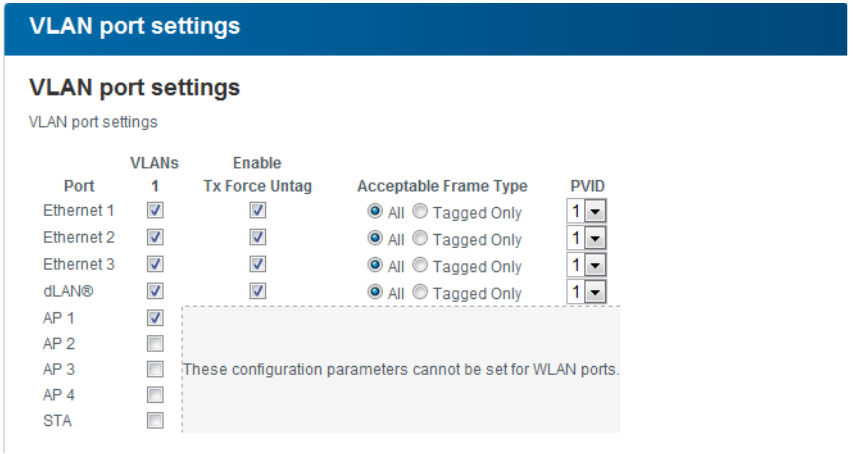
4.6.2 Overview of configured VLANs

To delete a VLAN, first enable it and then confirm with **Delete**. It is not possible to delete all VLANs; one VLAN must remain configured.

An enabled VLAN configuration requires at least one configured VLAN, since otherwise the configuration interface is no longer accessible and no connection of the port is enabled.

4.6.3 VLAN port settings

The VLAN port settings are configured here.

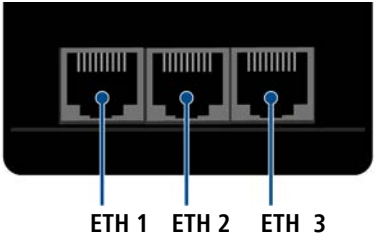


The existing ports of the dLAN pro 500 Wireless+ are listed in the first left column.

The configuration of the dLAN port is not available until future software versions.

The configured VLANs are listed in the row header. The ports can be assigned to the VLANs via the matrix.

Multiple VLANs can be assigned to the Ethernet ports and the dLAN port.



Wi-Fi ports can be assigned only to a VLAN.

For detailed information about this, refer to the online FAQs on our Internet site www.devolo.com.

If the Wi-Fi mode **Access point** is enabled, only the access points are assigned to the VLANs. If the Wi-Fi mode **WLAN client** is enabled, only the Wi-Fi client is assigned to the VLAN.

The behaviour of the port is configured via the columns **Force Tx Untag**, **Acceptable Rx Frame Types (All/ Tagged only)** and **Default VLAN (ID)**:

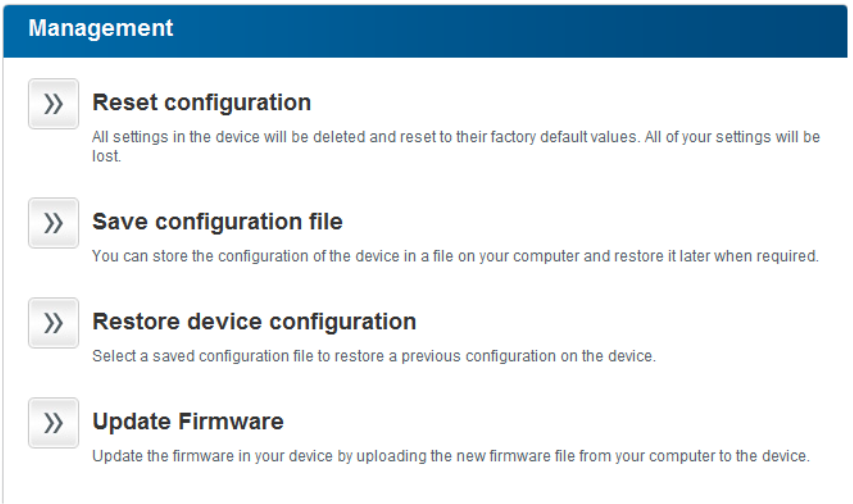
- If the option **Force Tx Untag** is enabled, all **outgoing frames** are sent from this port as **"untagged"**.
- If the option **Force Tx Untag** is **not** enabled, all **outgoing frames** are sent from this port as **tagged**.

  The **factory defaults** *of the dLAN pro 500 Wireless+* have the option **Force Tx Untag enabled***, i.e. all frames are sent "untagged".*

- The option **Acceptable Rx Frame Types (All/ Tagged only)** refers to the incoming data path of the ports. It determines whether all frames i.e. "tagged" and "untagged" (**All**) are accepted or only "tagged" frames (**Tagged Only**). If the **All** setting is enabled, all "untagged" frames are forwarded to the VLAN with the **Default VLAN (ID)** configured for this port.
- Under **Default VLAN (ID)**, the **VLAN ID** is specified, which is assigned to the **received "untagged"** frames. In the setting **Acceptable Rx Frame Types (Tagged only)**, the configured Default VLAN (ID) is insignificant.
- Under **Default Prio**, the **VLAN priority** is specified, which is assigned to the **received "untagged"** frames.

4.7 Management

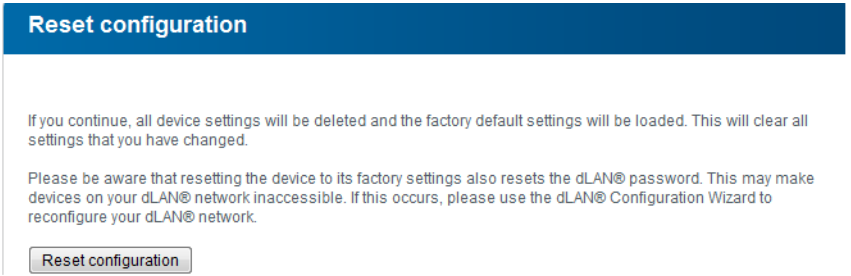
In the **Management** area you can reset the current configuration to the factory defaults, save it to your computer as a file or restore it from there and update the firmware of the dLAN pro 500 Wireless+.


Management
Reset configuration
All settings in the device will be deleted and reset to their factory default values. All of your settings will be lost.
Save configuration file
You can store the configuration of the device in a file on your computer and restore it later when required.
Restore device configuration
Select a saved configuration file to restore a previous configuration on the device.
Update Firmware
Update the firmware in your device by uploading the new firmware file from your computer to the device.

4.7.1 Resetting the configuration

With the **Management** ⇨ **Reset configuration** command, the dLAN pro 500 Wireless+ is reset to the original factory defaults. In doing so, you lose your personal settings.

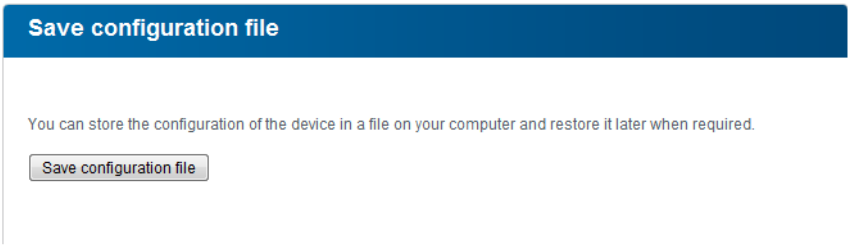
The last-assigned dLAN password for the dLAN pro 500 Wireless+ is also reset. To re-secure your dLAN pro network individually, read further at **4.4.3 dLAN settings**.


Reset configuration
If you continue, all device settings will be deleted and the factory default settings will be loaded. This will clear all settings that you have changed.
Please be aware that resetting the device to its factory settings also resets the dLAN® password. This may make devices on your dLAN® network inaccessible. If this occurs, please use the dLAN® Configuration Wizard to reconfigure your dLAN® network.
Reset configuration

For backup purposes, all enabled configuration settings can be transmitted to your computer, stored there as a file and reloaded into the dLAN pro 500 Wireless+. In this way, you can for example generate configurations for different network environments, with which you can set up the device quickly and easily.

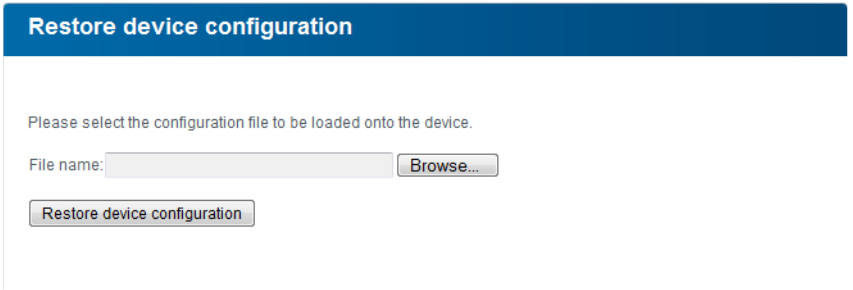
4.7.2 Saving a configuration file

To save the enabled configuration to your computer as a file, select the corresponding button in the area **Management** ▷ **Save configuration file**. Then enter a storage location and name for the settings file.


Save configuration file
You can store the configuration of the device in a file on your computer and restore it later when required.
Save configuration file

4.7.3 Restoring a configuration

An existing configuration file can be sent to the dLAN pro 500 Wireless+ in the area **Management** ⇨ **Restore device configuration** and enabled there. Select a suitable file via the **Browse…** button and start the operation by clicking the **Restore device configuration** button.


Restore device configuration
Please select the configuration file to be loaded onto the device.
File name:
Browse...
Restore device configuration

4.7.4 Update firmware

The firmware of the dLAN pro 500 Wireless+ includes the software for operating the device. If necessary, devolo offers new versions on the Internet as a file download, for example to modify existing functions.

① To bring the firmware up to the latest version, first go to the devolo website, www.devolo.com, and download the appropriate file for the dLAN pro 500 Wireless+ to your computer.

② Then in the configuration dialogue, go to the area **Management** ▷ **Update Firmware**. Click **Browse…** and select the downloaded file.

③ Then start the update procedure with the **Update Firmware** button. After a successful update, the dLAN pro 500 Wireless+ restarts automatically.

Ensure that the update procedure is not interrupted. To do so, it is best to connect your computer to the dLAN pro 500 Wireless+ via dLAN or LAN rather than Wi-Fi.

5 dLAN pro network

5.1 Security in the dLAN

Before you can use the dLAN pro 500 Wireless+ in your dLAN pro network, first you have to connect it to other dLAN pro devices as a home network. Two specific pieces of information are especially important for this:

- Shared use of the dLAN password serves as access control to the dLAN pro network and results in a delimited dLAN pro network.
- Shared use of a dLAN password serves as encryption of the dLAN pro network, and thereby the interception protection, of the transmitted data.

The dLAN password can be specified automatically via the encryption button or manually using the dLAN AVpro manager program. Please note the following basic principle when choosing your encryption method:

- In dLAN pro networks, data encryption is as simple as touching a button, since all corresponding dLAN pro devices are equipped with an encryption button.
- For dLAN pro networks that include devices with and without encryption buttons, data encryption must be set up using the dLAN AVpro manager.

5.2 dLAN pro network encryption at the touch of a button

To encrypt a dLAN pro network, in which all associated devices are equipped with an encryption button, simply press the encryption button that is located on the device. Pressing this button will encrypt your dLAN pro network with a randomly generated password.

For security reasons, the function of the encryption button can be disabled in the dLAN AVpro manager or on the configuration interface under 4.4 Device configuration***.***

The following section contains exact instructions of encryption on the basis of possible network scenarios:

Devices cannot be configured while in Standby mode.

Encrypting a new dLAN pro network with a dLAN pro 500 Wireless+ and an additional dLAN pro device

Once both dLAN pro devices have been successfully connected, press each encryption button for > one second within two minutes of one another.

That's it! Your dLAN pro network is now protected against unauthorised access.

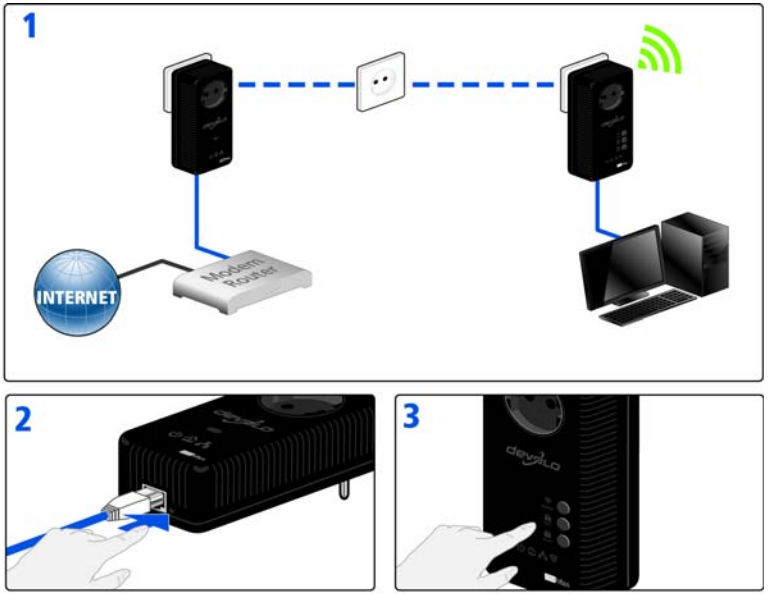


Fig. 9

Expanding an existing dLAN pro network by adding another dLAN pro device

If you have already secured your existing dLAN pro network using the encryption button, use the same method to integrate further devices. Once you have successfully connected the new dLAN pro device, first press the encryption button (> one second) of one of your network's existing devices, then press the encryption button (> one second) of your new dLAN pro device within two minutes.

That's it! The new dLAN pro device is now integrated in your network. To integrate additional dLAN pro devices in your network, repeat the above steps.

Fig. 10

Removing a dLAN pro device from a network

To remove a dLAN pro 500 Wireless+ or another dLAN pro device from an existing network, press its encryption button for at least ten seconds. The device will be assigned a new randomly generated password and will thus no longer be able to access the network.

To integrate the device into a different dLAN pro network, follow the steps described above, depending on whether you are setting up a new network or adding the device to an existing one.

Fig. 11

5.3 dLAN AVpro manager

The installation wizard installs the devolo dLAN AVpro manager configuration software as well as the associated manual on the Windows operating system (see 3.4.1 Software for Windows and Linux).

In addition to the individual encryption of your dLAN pro network and the security from unauthorised access, **devolo dLAN AVpro manager** offers other expanded dLAN functions.

For detailed descriptions and information on configuration of your dLAN pro network please consult this devolo dLAN AVpro manager manual.

6 Appendix

6.1 Bandwidth optimization

To significantly improve the transmission capacity of the network, we recommend that you comply with the following "connection rules":

- Plug the device directly into a wall socket. Avoid multiple sockets.
- You should connect all additional network devices that are connected to a multiple socket to the mains power supply via the electrical socket integrated into the dLAN pro 500 Wireless+.

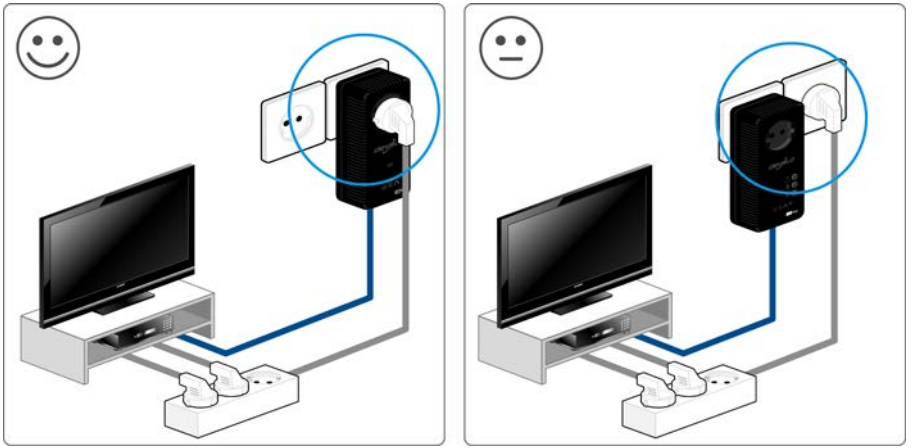


Fig. 12

For the permitted voltage range for operating the device and the power consumption, refer to the label on the rear side of the device. Additional technical information is available on the product sheet.

6.2 Important safety instructions

All safety and operating instructions should be read and understood before using the device, and should be kept for future reference.

- Never open the device. There are no user-serviceable parts inside the device.

Do not try to service this product yourself! Contact qualified technicians each and every time your device needs maintenance. There is a risk of electric shock!

- Use the device in a dry location only.

The outlet must be within reach of the connected network device. The product and the network device must be easily accessible.

- To switch the device off, pull the power plug out of the power outlet.
- To disconnect the device from the power supply grid, pull the power plug.
- Do not keep the device in direct sunlight.
- Do not insert any objects into the openings of the device.
- Slots and openings on the case serve as ventilation. Never block or cover them.
- Never set up the device near a heater or radiator.
- The device should be located only where sufficient ventilation can be ensured.
- Disconnect the device from the power supply grid before cleaning. Use a moist towel to clean the device. Never use water, paint thinner, benzene, alcohol or other strong cleaning agents when cleaning the device, as these could damage the case.
- Never use the device with a power supply that does not meet the specifications provided on the rating plate.
- In the event of damage, disconnect the device from the power supply grid and contact customer service. This applies, for example, if
  - the power cable or plug is damaged.

- liquid has been spilled on the device or objects have fallen into the device.
- the device has been exposed to rain or water.
- the device does not work, even though the operating instructions have been followed properly.
- the device's case is damaged.

6.3 Disposal of old devices

To be used in the countries of the European Union and other European countries with a separate collecting system:

The icon with crossed-out wastebasket on the device means that this adapter is an electrical or electronic device that falls within the scope of application of the German Electrical and Electronic Equipment Act ("Elektrogesetz"). Since 24 March 2006, these types of devices may no longer be disposed of with household waste. Rather, in Germany, they can be given to a municipal collection point free of charge. Contact your municipal government to find out the address and hours of the nearest collection point.

6.4 Warranty conditions

The devolo AG warranty is given to purchasers of devolo products in addition to the warranty conditions provided by law and in accordance with the following conditions:

1 Warranty coverage

a) The warranty covers the equipment delivered and all its parts. Parts will, at devolo's sole discretion, be replaced or repaired free of charge if, despite proven proper handling and adherence to the operating instructions, these parts became defective due to fabrication and/or material defects. Alternatively, devolo reserves the right to replace the defective product with a comparable product with the same specifications and features. Operating manuals and possibly supplied software are excluded from the warranty.

b) Material and service charges shall be covered by devolo, but not shipping and handling costs involved in transport from the buyer to the service station and/or to devolo.

c) Replaced parts become property of devolo.

d) devolo is authorized to carry out technical changes (e.g. firmware updates) beyond repair and replacement of defective parts in order to bring the equipment up to the current technical state. This does not result in any additional charge for the customer. A legal claim to this service does not exist.

2 Warranty period

The warranty period for this devolo product is three years. This period begins at the day of delivery from the devolo dealer. Warranty services carried out by devolo do not result in an extension of the warranty period nor do they initiate a new warranty period. The warranty period for installed replacement parts ends with the warranty period of the device as a whole.

3 Warranty procedure

a) If defects appear during the warranty period, the warranty claims must be made immediately, at the latest within a period of 7 days.

b) In the case of any externally visible damage arising from transport (e.g. damage to the housing), the person carrying out the transportation and the sender should be informed immediately. On discovery of damage which is not externally visible, the transport company and the sender are to be immediately informed in writing, at the latest within 3 days of delivery.

c) Transport to and from the location where the warranty claim is accepted and/or the repaired device is exchanged, is at the purchaser's own risk and cost.

d) Warranty claims are only valid if a copy of the original purchase receipt is returned with the device. devolo reserves the right to require the submission of the original purchase receipt.

4 Suspension of the warranty

All warranty claims will be deemed invalid

a) if the label with the serial number has been removed from the device,

b) if the device is damaged or destroyed as a result of acts of nature or by environmental influences (moisture, electric shock, dust, etc.),

c) if the device was stored or operated under conditions not in compliance with the technical specifications,

d) if the damage occurred due to incorrect handling, especially to non-observance of the system description and the operating instructions,

e) if the device was opened, repaired or modified by persons not contracted by devolo,

f) if the device shows any kind of mechanical damage, or

g) if the warranty claim has not been reported in accordance with 3a) or 3b).

5 Operating mistakes

If it becomes apparent that the reported malfunction of the device has been caused by unsuitable hardware, software, installation or operation, devolo reserves the right to charge the purchaser for the resulting testing costs.

6 Additional regulations

The above conditions define the complete scope of devolo's legal liability.

a) The warranty gives no entitlement to additional claims, such as any refund in full or in part. Compensation claims, regardless of the legal basis, are excluded. This does not apply if e.g. injury to persons or damage to private property are specifically covered by the product liability law, or in cases of intentional act or culpable negligence.

b) Claims for compensation of lost profits, indirect or consequential detriments, are excluded.

c) devolo is not liable for lost data or retrieval of lost data in cases of slight and ordinary negligence.

d) In the case that the intentional or culpable negligence of devolo employees has caused a loss of data, devolo will be liable for those costs typical to the recovery of data where periodic security data back-ups have been made.

e) The warranty is valid only for the first purchaser and is not transferable.

f) The court of jurisdiction is located in Aachen, Germany in the case that the purchaser is a merchant. If the purchaser does not have a court of jurisdiction in the Federal Republic of Germany or if he moves his domicile out of Germany after conclusion of the contract, devolo's court of jurisdiction applies. This is also applicable if the purchaser's domicile is not known at the time of institution of proceedings.

g) The law of the Federal Republic of Germany is applicable. The UN commercial law does not apply to dealings between devolo and the purchaser.

Index

C
CE declaration 8

D
Default Wi-Fi key 21, 46, 53, 61
devolo dLAN AVpro manager 24, 75
DHCP server 34
Disposal of old devices 79
dLAN encryption 35
dLAN password 35
dLAN pro network 71

E
Encryption button 71

I
Important safety instructions 78
Indicator lights 19
IP address 33

L
LAN (Network connection) 23

M
MAC address 50
Multi-SSID 46

P
Package contents 18
Parental controls 43

R
RADIUS server 43
Rented offices 14
Reset 22

S
Security ID 21
Software installation 24
SSID 48
System requirements 18

T
tagged 65
Time server 37

U
untagged 65

V
VLAN 61
VLAN ID 63
VLAN port 64

W
Warranty 79
WEP 52, 61

Wi-Fi access point 28
Wi-Fi antenna 23
Wi-Fi client 39
Wi-Fi filter 49
Wi-Fi key 46
WiFi Move Technology 45
Wi-Fi ON/OFF button 21
Wi-Fi Protected Setup (WPS) 22, 56
Wi-Fi time control 42
WPA 61
WPA/WPA2 Enterprise Mode 53, 61
WPA/WPA2 Private Mode 53